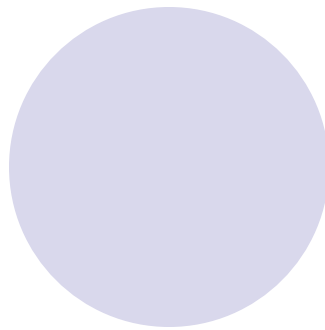
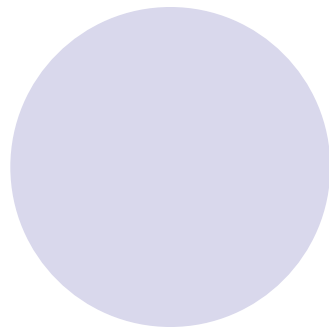


# myVocs : Cross Domain Authorization For Federated Virtual Organizations



Jill Gemmill

John-Paul Robinson

University of Alabama at Birmingham

April 2006

# Acknowledgments



- **NSF ANI-0330543** NMI Enabled Open Source Collaboration Tools for Virtual Organizations (Gemmill, **John-Paul Robinson**)
- **N01-LM-3-3513** Advanced Network Infrastructure for Health & Disaster Management (Orthner, Terndrup, Grimes, Gemmill)
- **Office of the VPIT** and IT Academic Computing
- **Von Welch, Tom Scavo- NCSA/UIUC**
- **Internet2** MACE and MLIST Working Group members
- Serge Aumont, Olivier Salaun, **CRU**
- Members of MACE-MLIST Working Group

# What's a Virtual Organization?

- A set of collaborators bound together by a project of common interest
  - very large scale science projects eg: Teragrid
  - Half a dozen or so collaborators in a funded multidisciplinary project
  - Physicians at 60 cancer centers wanting to share clinical data to increase N or focus on special sub-populations
  - An Internet2 Working Group; a conference planning committee.
- In general, VO members are from different institutions



Problem

- What system architecture is required to support cross-domain single sign-on for Virtual Organizations?

- IDENTITY

- How many separate logins for services on the Internet do you have?

# Approaches to Cross-Domain AAA: Grid Computing and Federations

- **Grids** (*Foster, Kesselman*)

- Purpose: to support research VO's
- Implementation: **NMI GRIDS Globus Toolkit**
- PKI based security infrastructure uses **X.509 Certificate** (ITU-T, IETF standard)
  - Contains some Distinguished Name
  - Keys distributed to each end user
- Authorization will be dealt with later

- **Federations** (*SAML, Shibboleth, WS-Security*)

- Purpose: mostly business driven B2B
- EDIT approach uses **Assertions** XML, digitally signed assertions, bindings to services eg: SOAP
- Implementation: **NMI EDIT eduPerson, Shibboleth**
- Authorization cannot be done without Authentication (attribute assertions)
  - Security Assertion Markup Language (XML) : Highly flexible assertion content
  - Server Level X.509 Certs used for secure communication channels <sup>5</sup> and assertion signatures

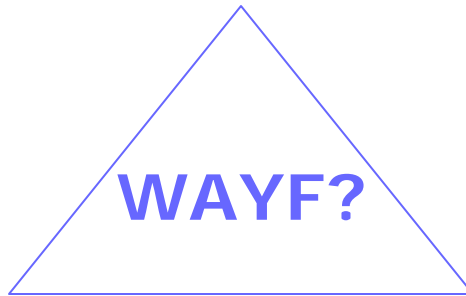
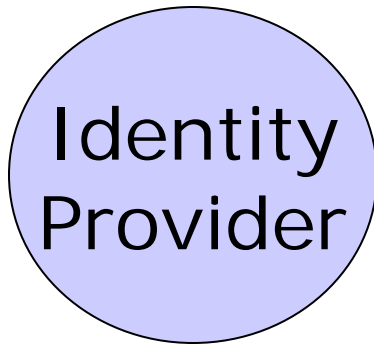
Don't These Solutions Provide What Is Needed by VO's? No!

- Single Domain solutions inadequate
- Most collaboration tools accessed by web browser (not client software w. certificate)
- Essential VO (Group) Membership information not provided consistently by either one
- VO-based Federation

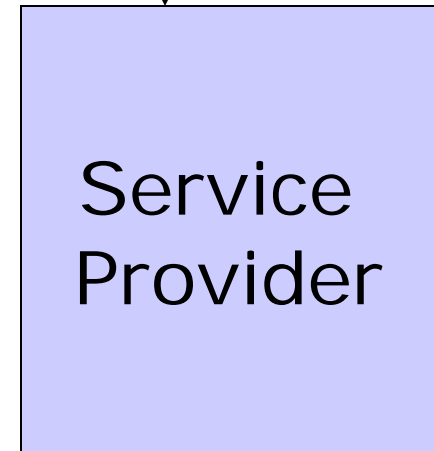
# What does Shibboleth bring to the table?

- A large (and growing) international installed base
- A standards-based, open source implementation
- Working SAML 1.1 code
- A standard attribute vocabulary (eduPerson)
- A well-developed, federated identity management infrastructure has sprung up around Shibboleth

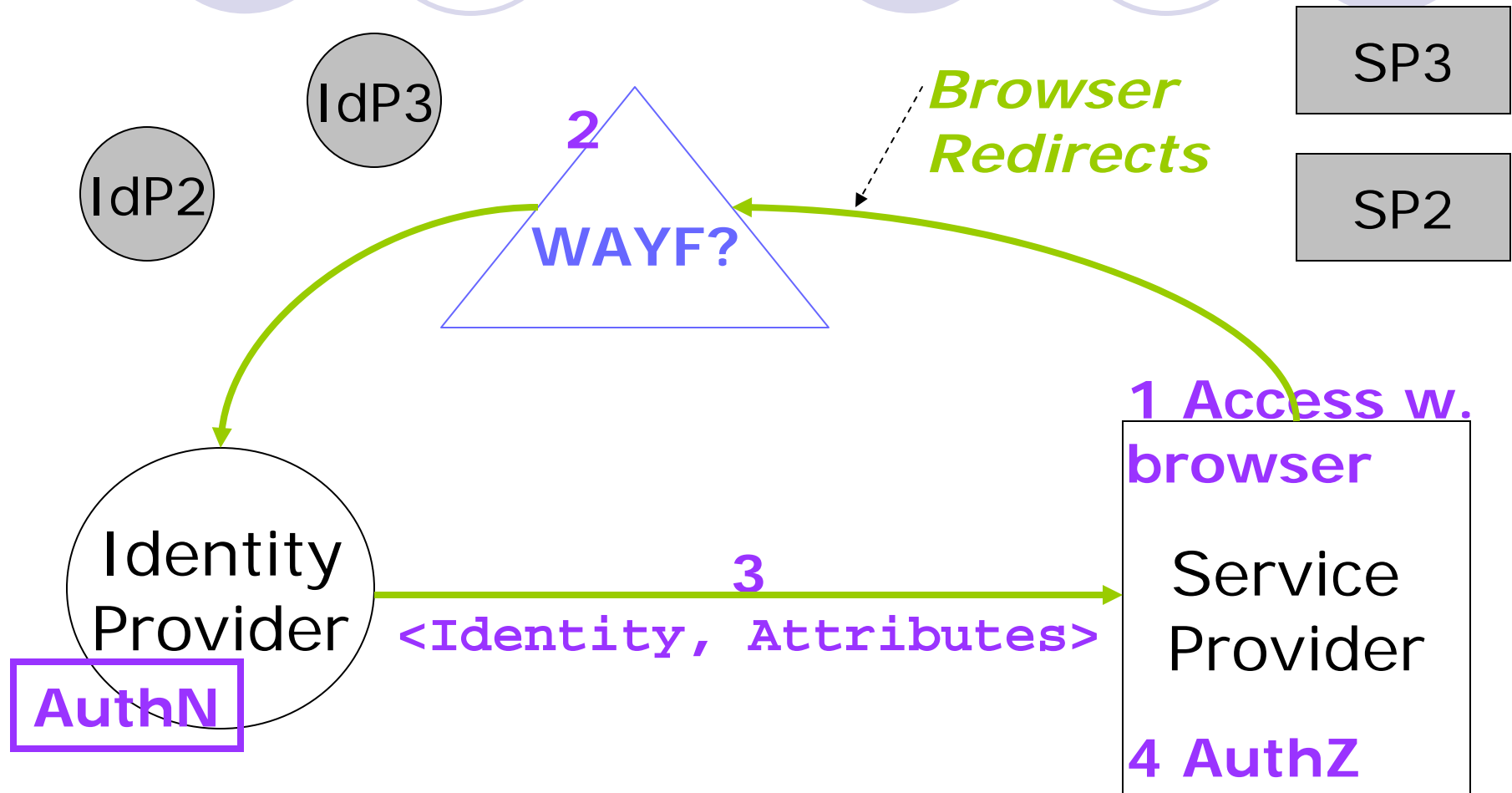
# Introduction to Shibboleth



*Start here*



# Introduction to Shibboleth



# Motivations



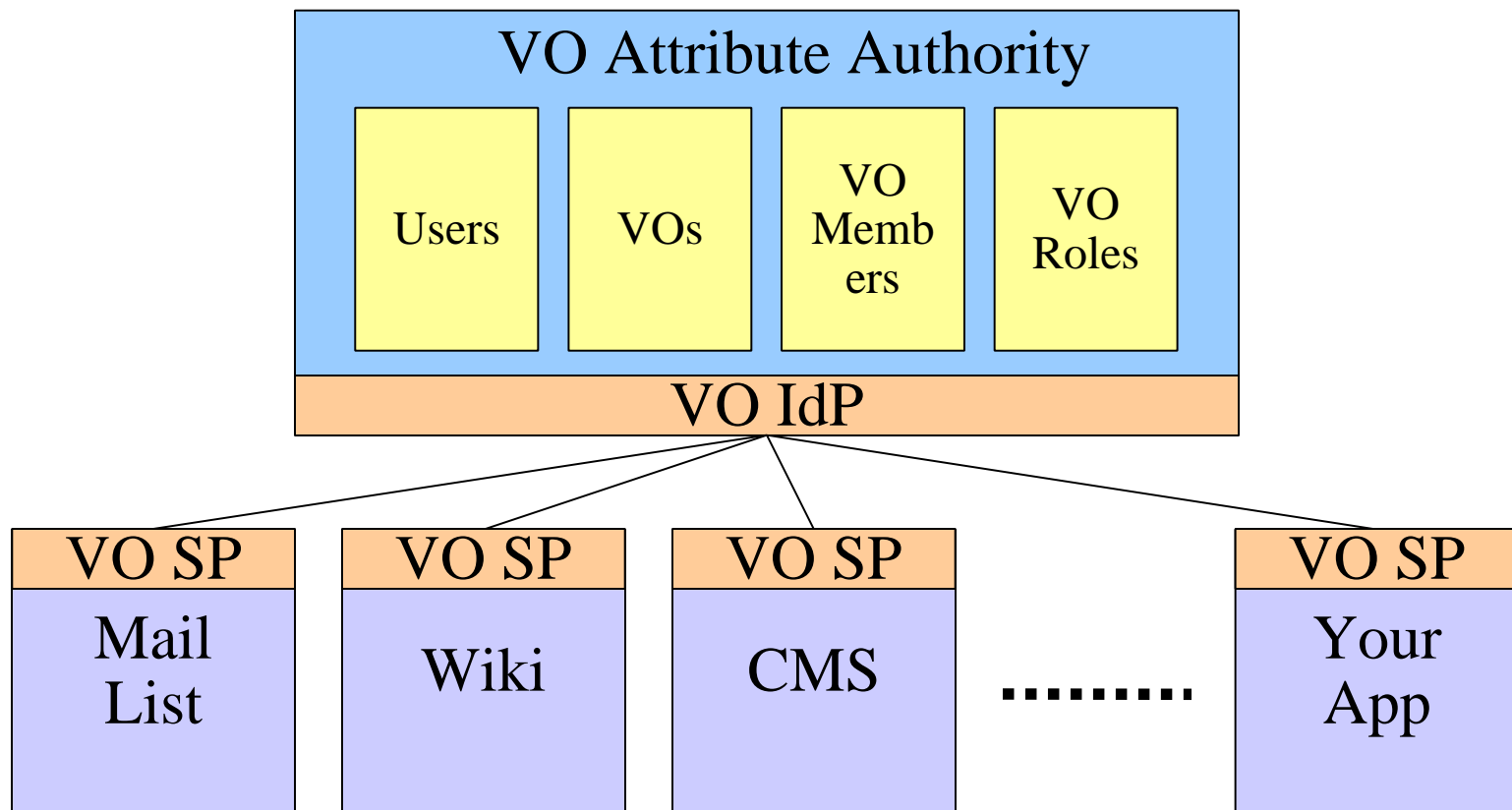
- Leverage distributed identity mgt. infrastructure
- ATTRIBUTE based access control AT RESOURCE PROVIDER
- The most important attribute for VOs is: “member of VO-XYZ”
  - Who is authoritative for VO attributes?
  - How are VO attributes created?
  - Where are VO attributes stored?

# myVocs : my VO Collaboration System

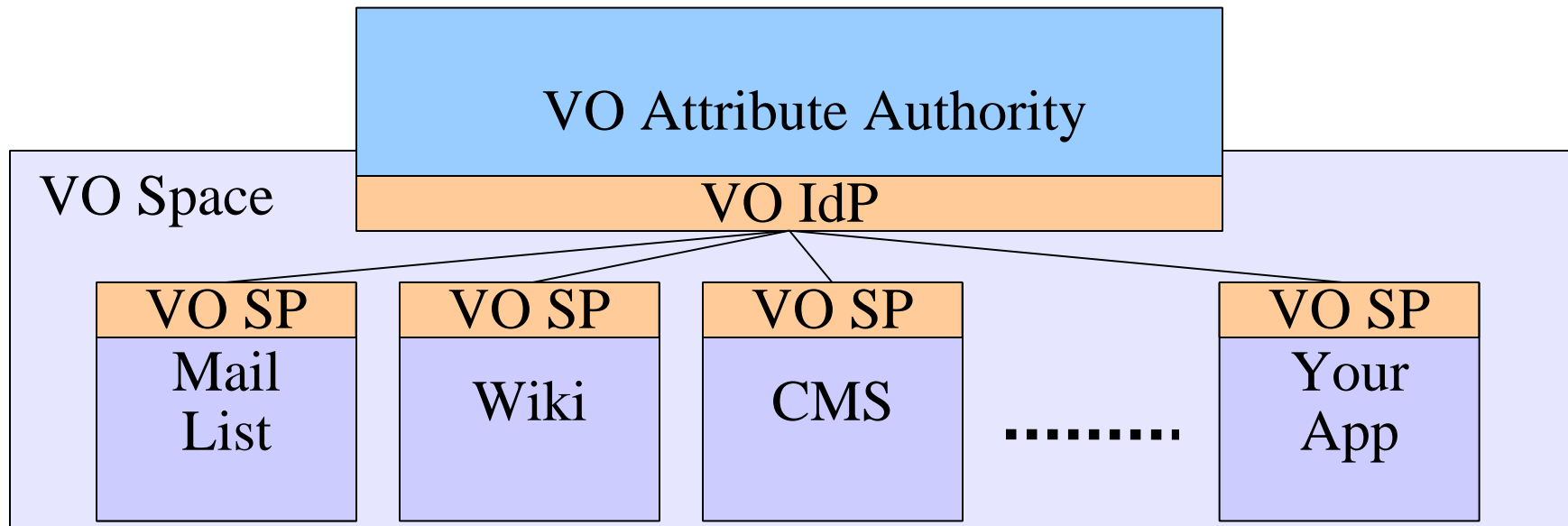
*lets you create and manage VOs*

- What is a collaboration system?
  - It depends on who's collaborating
  - Therefore, modularity is key
- “Typical” Tools
  - Mailing List (Sympa)
  - File Sharing (WebInsta)
  - Wiki (Joint content creation)  
PHPWiki
  - CMS (drupal)

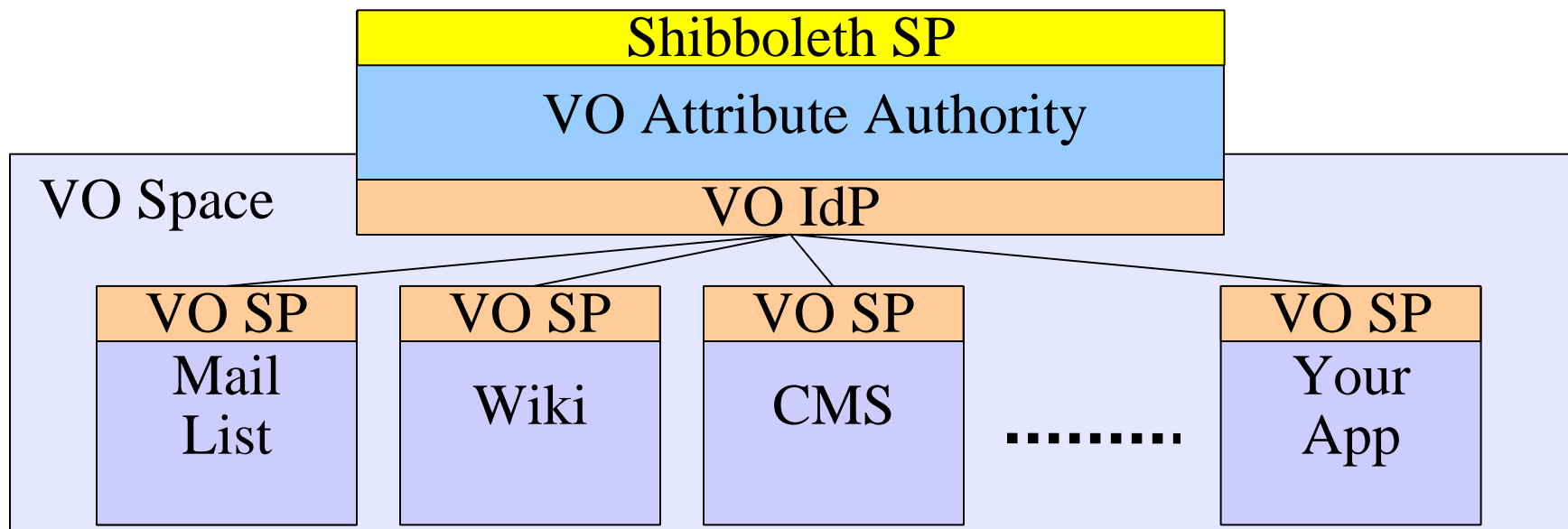
# A Look Inside myVocs



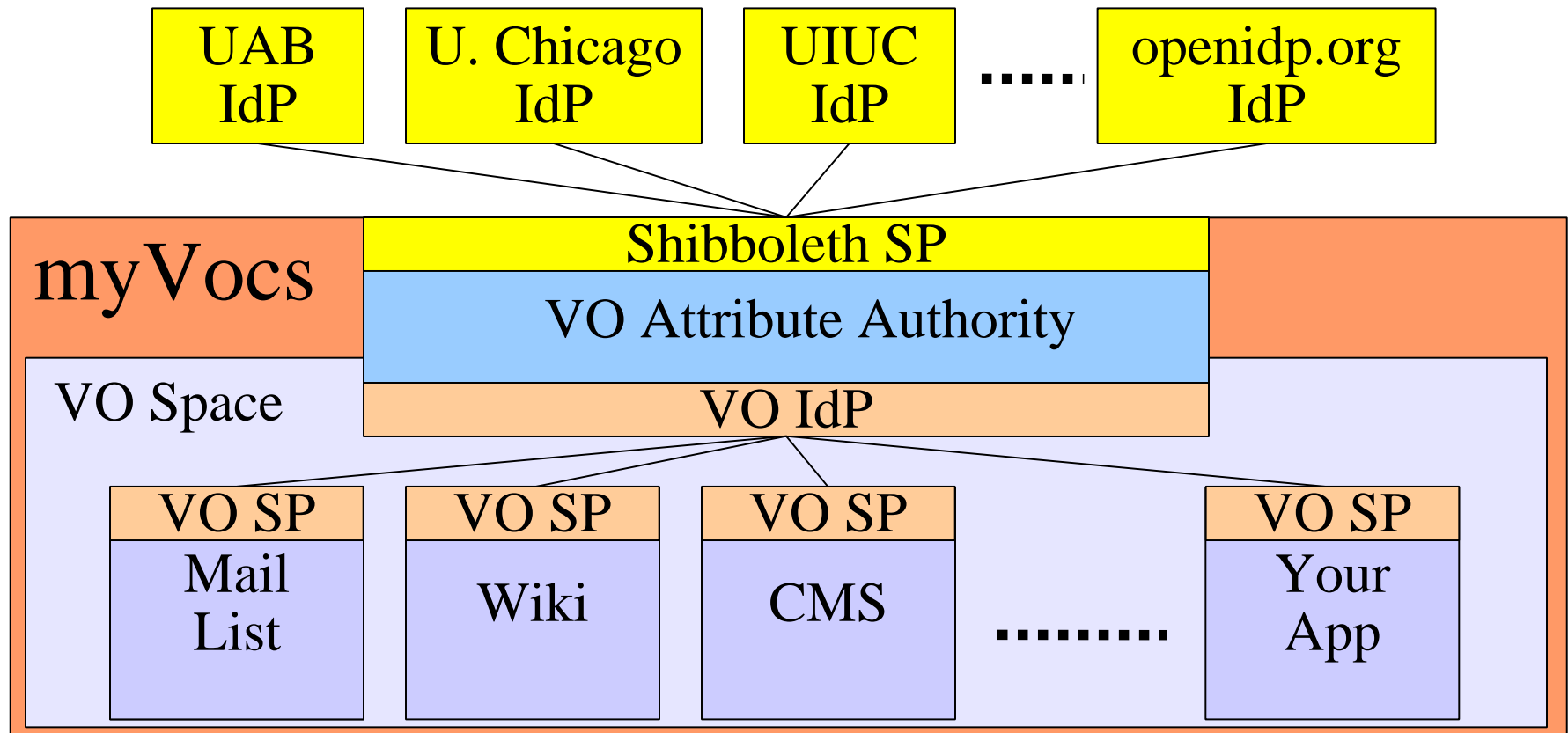
# A Look Inside myVocs



# A Look Inside myVocs



# A Look Inside myVocs





# myVocs automatically provisions

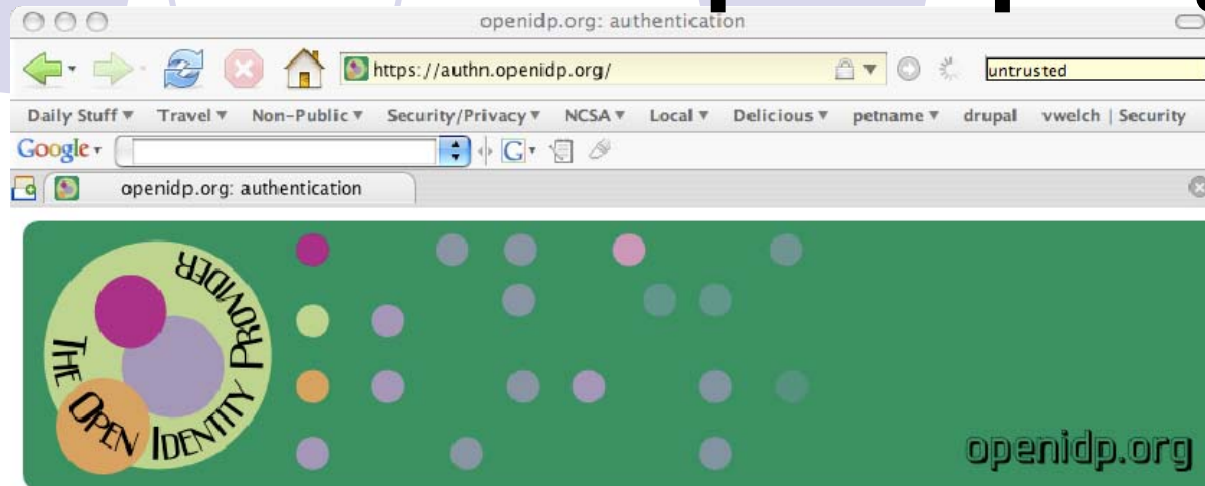
- Application Instances

- (one set per VO)

- **Accounts**

- Based on VO membership and roles

# openidp.org



Welcome to the openidp.org authentication service.  
Please provide your User ID and password to identify yourself.

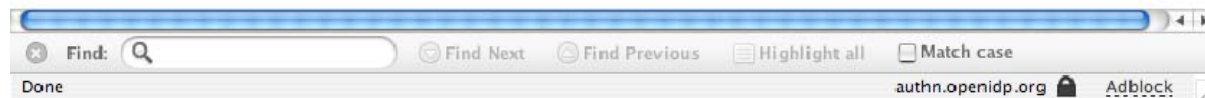
User ID

Password

Login gives you 8-hour access without repeat login to Shibboleth-protected Web resources.

**WARNING: Protect your privacy! Prevent unauthorized use!**  
Completely exit your Web browser when you are finished.

Copyright © 2005 openidp.org



# What is GridShib?

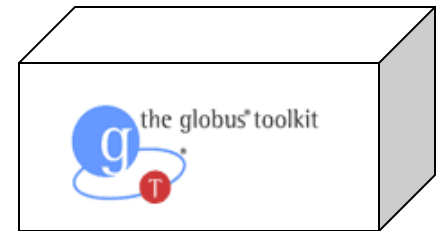
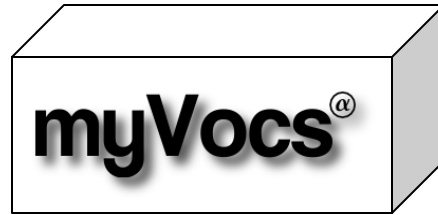
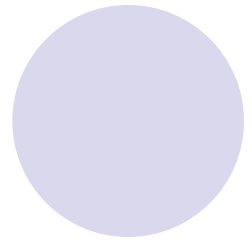
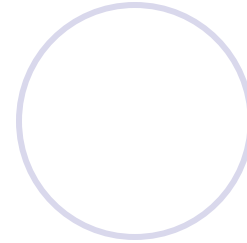
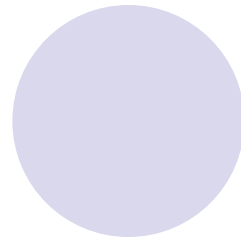
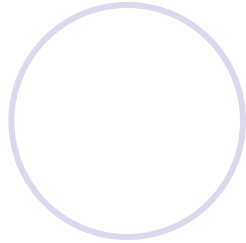
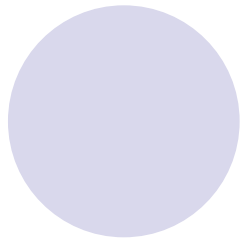


- GridShib enables *secure attribute sharing* among *Grid virtual organizations* and *higher-educational institutions*
- The goal of GridShib is to integrate the Globus Toolkit® with Shibboleth®
- GridShib adds *attribute-based authorization* to Globus Toolkit

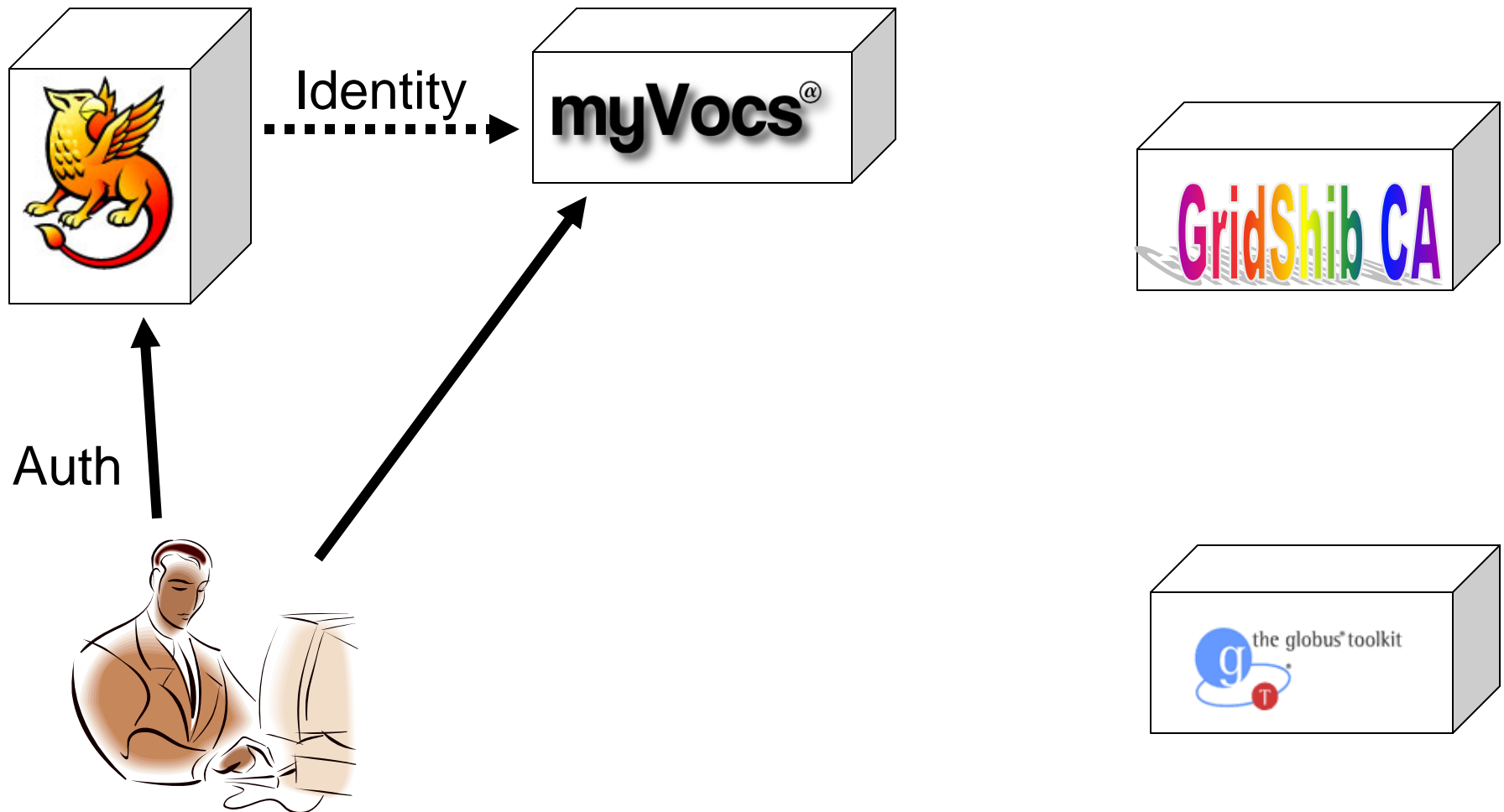


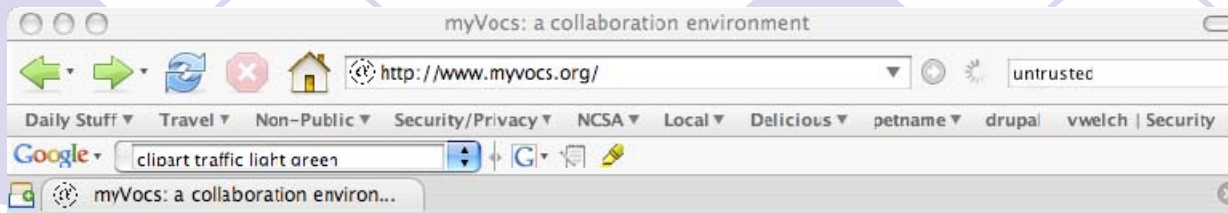
# myVocs-GridShib Integration

- GridShib enables *secure attribute sharing* among *Grid virtual organizations* and *higher-educational institutions*
- The goal of GridShib is to integrate the Globus Toolkit® with Shibboleth®
- GridShib adds *attribute-based authorization* to Globus Toolkit



# User Registers with myVocs





# myVocs<sup>α</sup>

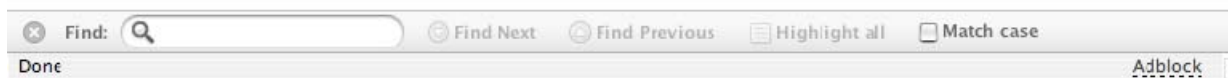
[Browse](#) [Project](#) [About](#)

Type in a command, or "ls" to show a list of all commands

Some examples of what you can do with myVocs:

- [cms collabtools](#) Open the CMS tool for the collabtools VO
- [wiki collabtools](#) Open the wiki for the collabtools VO
- [join collab:ools](#) Join the collabtools VC
- [tec wag\\_edu](#) Browse technocrati wag\_edu tags
- [del wag\\_edu](#) Browse del.icio.us wag\_edu tags
- [ls](#) List all available commands

[What Is This Tool?](#) | [Advanced Syntax](#)



InQueue: Identity Provider Selection

https://wayf.internet2.edu/InQueue/WAYF?shire=htt

Daily Stuff Travel Non-Public Security/Privacy NCSA Local Delicious petname drupal vwelch Security

Google

InQueue: Identity Provider Selection

### Select an Identity Provider

In order to fulfill the request for a web resource you have just attempted to access, information must be obtained from your identity provider. Please select the provider with which you are affiliated.

**Choose from a list:**

AAI EDUHR TEST Select Remember for session

or

**Search by keyword:**

Search

Search results:

- openidp.org | The Open Identity Provider
- openidp.org | The Open Identity Provider (shib13)

Select Remember for session

Find out about [InQueue](#).

Got here by mistake? Don't see a suitable or recognizable identity provider in the list? Just use your browser's Back button to return to the page that sent you here.



INTERNET<sup>2</sup> Shibboleth<sup>®</sup>

Find: Find Next Find Previous Highlight all Match case


http://incueue.internet2.edu/ wayf.internet2.edu AdBlock

Weblogin: login page - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Print Mail News RSS Feeds

Address <https://weblogin.ac.uab.edu/> Go Links



The resource you requested requires you to authenticate.


BlazerID


Password

Weblogin Single Sign-on gives you 8-hour access without repeat login to protected Web resources.

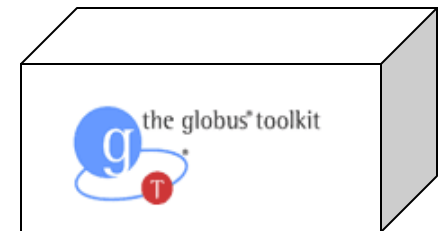
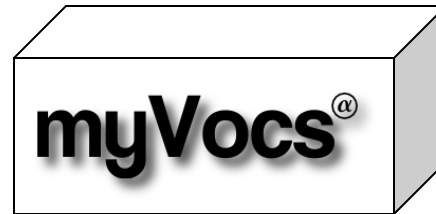
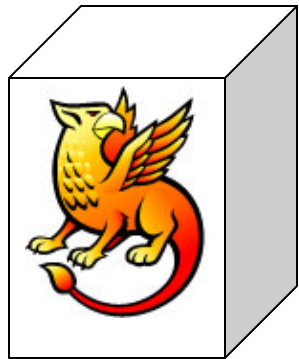
**WARNING:** Protect your privacy! Prevent unauthorized use!  
Completely exit your Web browser when you are finished.

[A WebISO Pilot Project by IT Academic Computing](#)





# VO Admin Adds User to VO



file Edit View Favorites Tools Help

Back Search Favorites

address http://webapp.lab.ac.uab.edu/sympa/review/gsmv Go Links

Logout [Create list](#) [Preferences](#) [Your subscriptions](#) [Home](#) [Help](#)

jgemmill@uab.edu Owner

## gsmv@webapp.lab.ac.uab.edu

Discussions of GridShib integration with myVocs

### List Administration Panel

[Subscribers](#) [Edit List Config](#) [Moderate](#) [Customizing](#) [Manage Archives](#) [Bounces](#) [Restore shared](#) [Remove List](#) [Rename List](#)

quiet

[Pending subscriptions](#) [Multiple add](#) [Remind all subscribers](#)

quiet Page size 25 page 1 / 1

X	Email	Domain	Name	Reception	Sources	Sub date	Last update
<input type="checkbox"/>	<a href="mailto:jgemmill@uab.edu">jgemmill@uab.edu</a>		Jill B Gemmill	mail	subscribed	22 Feb 2006	22 Feb 2006
<input type="checkbox"/>	<a href="mailto:jpr@uab.edu">jpr@uab.edu</a>			mail	subscribed	22 Feb 2006	22 Feb 2006
<input type="checkbox"/>	<a href="mailto:ndk@internet2.edu">ndk@internet2.edu</a>			mail	subscribed	24 Mar 2006	24 Mar 2006
<input type="checkbox"/>	<a href="mailto:tbarton@uchicago.edu">tbarton@uchicago.edu</a>		Tom Barton	mail	subscribed	22 Feb 2006	22 Feb 2006
<input type="checkbox"/>	<a href="mailto:trscavo@gmail.com">trscavo@gmail.com</a>		Tom Scavo	mail	subscribed	22 Feb 2006	22 Feb 2006
<input type="checkbox"/>	<a href="mailto:vwelch@ncsa.uiuc.edu">vwelch@ncsa.uiuc.edu</a>		Von Welch	mail	subscribed	22 Feb 2006	22 Feb 2006

quiet page 1 / 1

Done Internet

Logout

[Create list](#) [Preferences](#) [Your subscriptions](#) [Home](#) [Help](#)

jgemmill@uab.edu  
Owner

## gsmv@webapp.lab.ac.uab.edu

Discussions of GridShib integration with myVocs

### List Administration Panel

[Subscribers](#) [Edit List Config](#) [Moderate](#) [Customizing](#) [Manage Archives](#) [Bounces](#) [Restore shared](#) [Remove List](#) [Rename List](#)

quiet

[Pending subscriptions](#) [Multiple add](#) [Remind all subscribers](#)

quiet Page size 25 page 1 / 1

X	Email	Domain	Name	Reception	Sources	Sub date	Last update
<input type="checkbox"/>	<a href="mailto:jgemmill@uab.edu">jgemmill@uab.edu</a>		Jill B Gemmill	mail	subscribed	22 Feb 2006	22 Feb 2006
<input type="checkbox"/>	<a href="mailto:jpr@uab.edu">jpr@uab.edu</a>			mail	subscribed	22 Feb 2006	22 Feb 2006
<input type="checkbox"/>	<a href="mailto:ndk@internet2.edu">ndk@internet2.edu</a>			mail	subscribed	24 Mar 2006	24 Mar 2006
<input type="checkbox"/>	<a href="mailto:tbarton@uchicago.edu">tbarton@uchicago.edu</a>		Tom Barton	mail	subscribed	22 Feb 2006	22 Feb 2006
<input type="checkbox"/>	<a href="mailto:trscavo@gmail.com">trscavo@gmail.com</a>		Tom Scavo	mail	subscribed	22 Feb 2006	22 Feb 2006
<input type="checkbox"/>	<a href="mailto:vwelch@ncsa.uiuc.edu">vwelch@ncsa.uiuc.edu</a>		Von Welch	mail	subscribed	22 Feb 2006	22 Feb 2006

quiet page 1 / 1

List info

Subscribers: 6

Owners [jpr@uab.edu](mailto:jpr@uab.edu)  
Moderators  
[jgemmill@uab.edu](mailto:jgemmill@uab.edu)  
[ndk@internet2.edu](mailto:ndk@internet2.edu)  
[tbarton@uchicago.edu](mailto:tbarton@uchicago.edu)  
[trscavo@gmail.com](mailto:trscavo@gmail.com)  
[vwelch@ncsa.uiuc.edu](mailto:vwelch@ncsa.uiuc.edu)

List admin

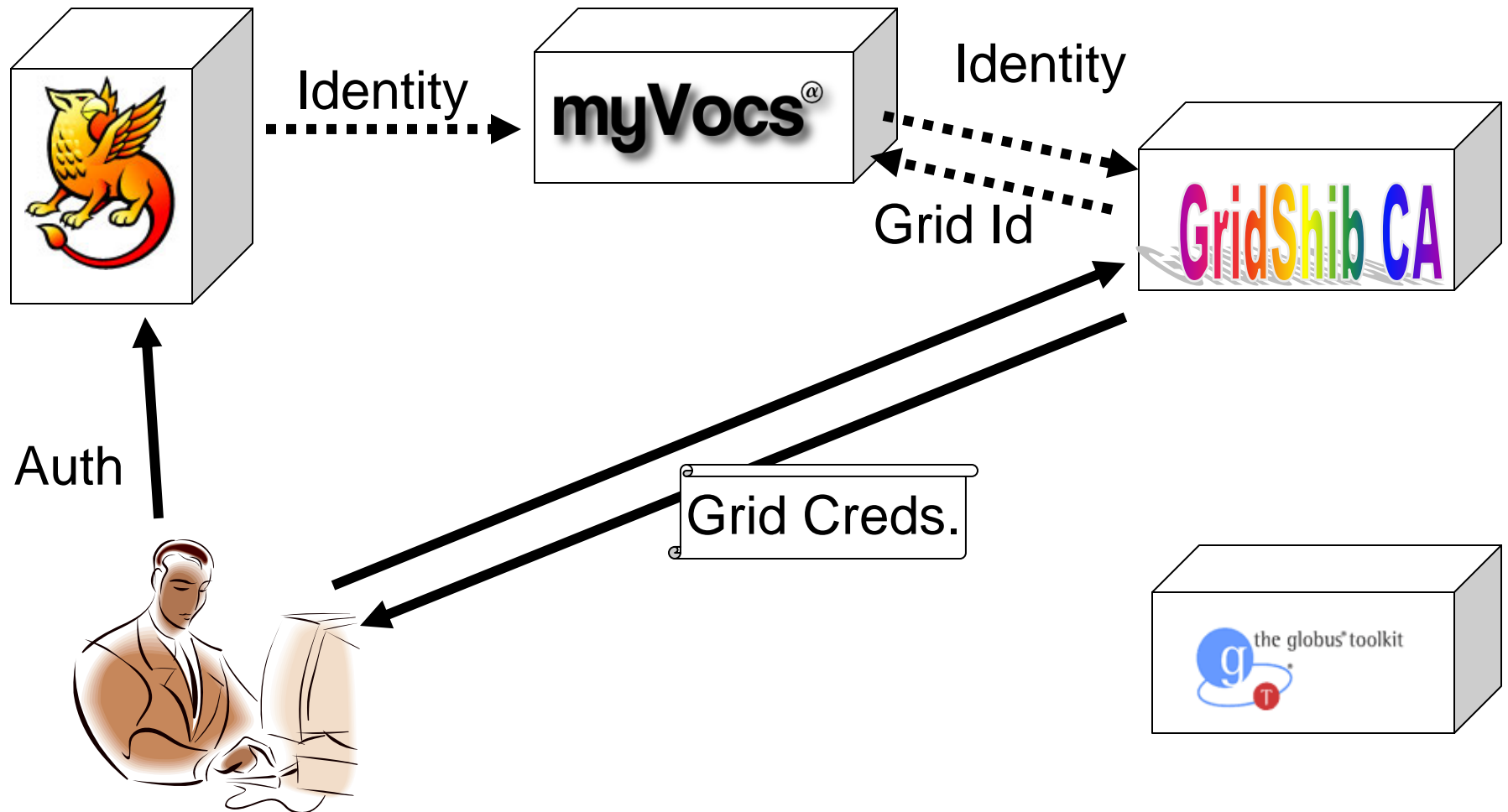
Bounced email rate: 0%

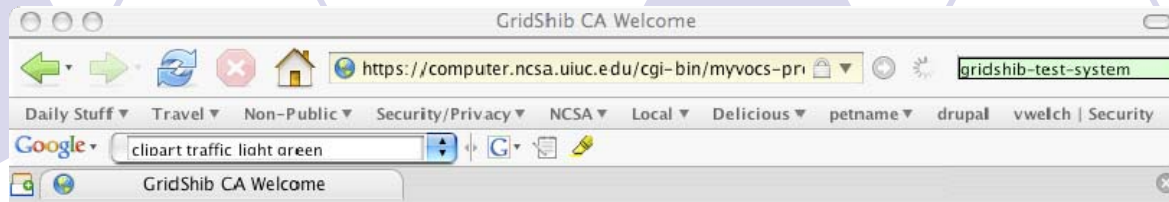
No message to moderate

Subscriber Options

Unsubscribe

# Grid Logon





## GridShib CA

(Version 0.1.5-test)  
[GridShib Home Page](#)



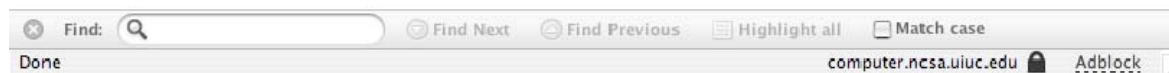
Welcome vwelch@openidp.org.

Your GridShib-CA identity will be /C=US/O=NCSA-TEST/OU=User//CN=vwelch@openidp.org

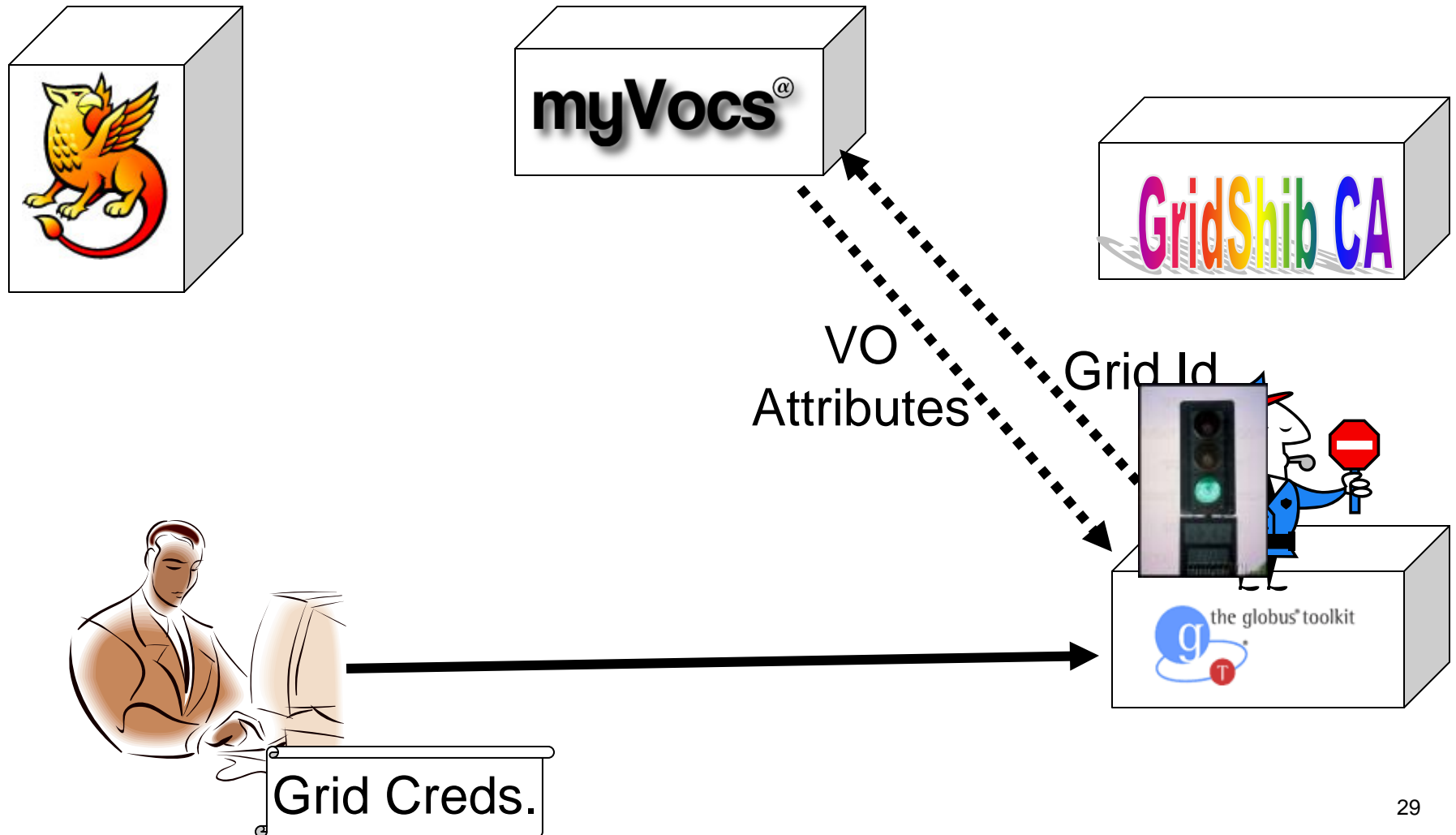
[Press here to generate and download Grid credential.](#)

---

Copyright 2006 The Board of Trustees of the University of Illinois.



# Grid Service Invocation



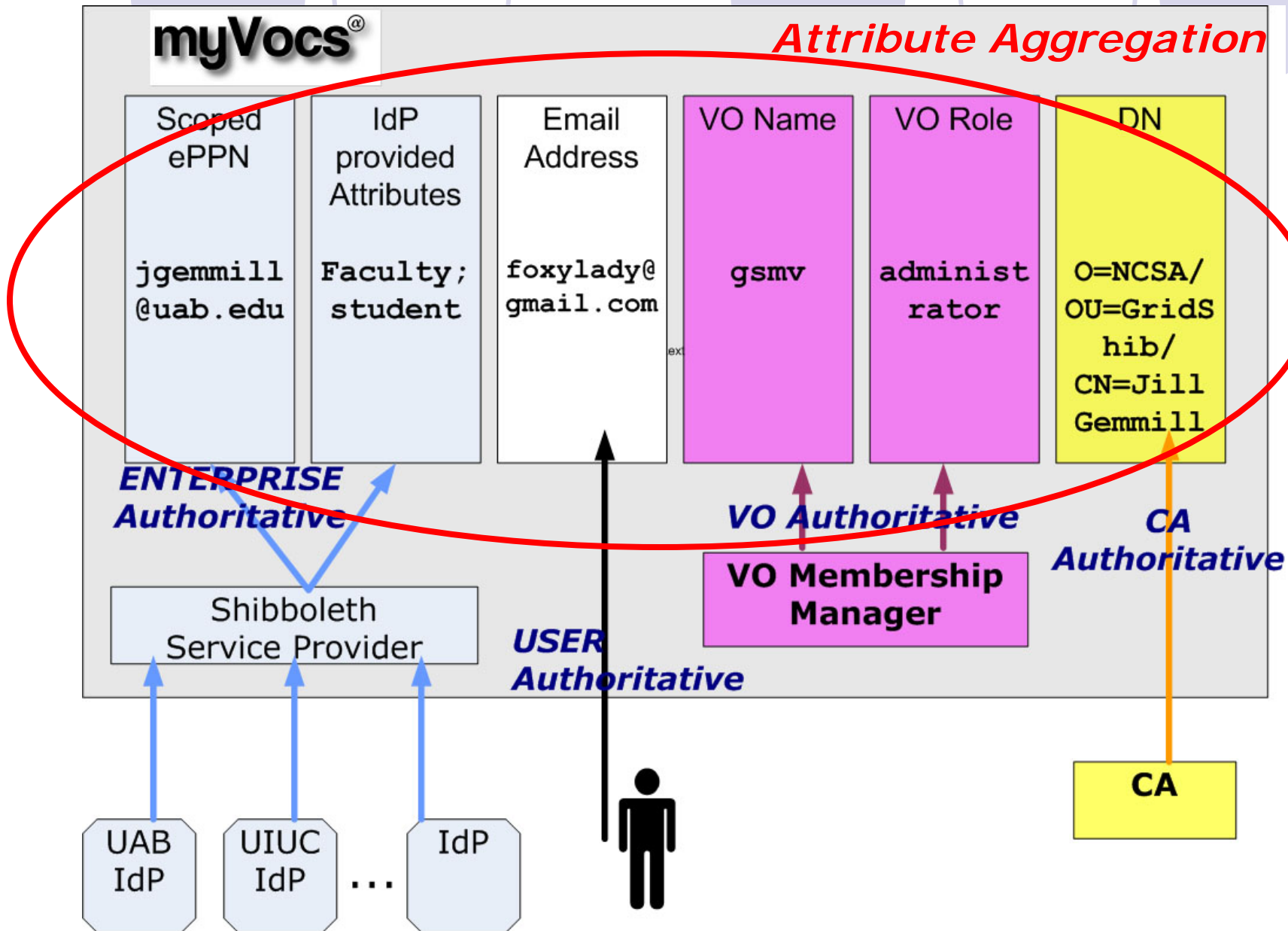
```
Default
New Configure
1: Default 2: Default
(von-mac) /usr/local/gt-4.0.1/bin>shibecho -s https://41.142.234.19:8443/wsrf/services/ShibEchoService
-----
Response:
-----

SAMLAttribute
{
  name= 'urn:mace:dir:attribute-def:role'
  namespace= 'urn:mace:shibboleth:1.0:attributeNamespace:uri'
  value #1 = 'editor@gsmv'
  value #2 = 'member@gsmv'
  :ssuer= 'https://idp.myvocs.org/shibboleth'
  notBefore= '2006-04-22T23:48:55Z'
  notOnOrAfter= '2006-04-23T07:48:55Z'
}SAMLAttribute
{
  name= 'urn:mace:dir:attribute-def:email'
  namespace= 'urn:mace:shibboleth:1.0:attributeNamespace:uri'
  value #1 = 'vwelch@ncsa.uiuc.edu'
  :ssuer= 'https://idp.myvocs.org/shibboleth'
  notBefore= '2006-04-22T23:48:55Z'
  notOnOrAfter= '2006-04-23T07:48:55Z'
}SAMLAttribute
{
  name= 'urn:mace:dir:attribute-def:uid'
  namespace= 'urn:mace:shibboleth:1.0:attributeNamespace:uri'
  value #1 = 'vwelch@openidp.org'
  :ssuer= 'https://idp.myvocs.org/shibboleth'
  notBefore= '2006-04-22T23:48:55Z'
  notOnOrAfter= '2006-04-23T07:48:55Z'
}SAMLAttribute
{
  name= 'urn:mace:dir:attribute-def:eduPersonPrincipalName'
  namespace= 'urn:mace:shibboleth:1.0:attributeNamespace:uri'
  value #1 = 'vwelch@openidp.org'
  :ssuer= 'https://idp.myvocs.org/shibboleth'
  notBefore= '2006-04-22T23:48:55Z'
  notOnOrAfter= '2006-04-23T07:48:55Z'
}

User names:
0 : echoUser
1 : tester1

(von-mac) /usr/local/gt-4.0.1/bin>
```

# Inside myVocs





# Questions?

- Jill Gemmill

- [jgemmill@uab.edu](mailto:jgemmill@uab.edu)

