

# Shibboleth & Grid Integration

STFC and University of Oxford  
(and University of Manchester)



# Acknowledgements

- Slides by David Spence
- ShibGrid (University of Oxford + STFC)
- SARoNGS (STFC, University of Oxford, University of Manchester)



# Overview

- Motivation – Grid
- Why Shibboleth?
- Previous work: ShibGrid
- Other projects
- Just starting: SARoNGS



# Background

- UK National Grid Service
  - Production Grid since 2004
- Operations Support Centre based at STFC RAL
  - CA, MyProxy, RB, Helpdesk ...

# Motivation - Grid

- We want to encourage more (academic) users to use the Grid
  - All areas of research
  - Single researcher to large projects
  - Security infrastructure must enable this
    - PKI often a barrier
    - X.509: Currently generalised solution for all
    - Must be straightforward to use



# Why Shibboleth?

- JISC is encouraging all institutions to transition from Athens to “Federated Access Management”
- This technology is based on Shibboleth
- This will become familiar to all academic users
- The Grid should also use this common technology for authentication

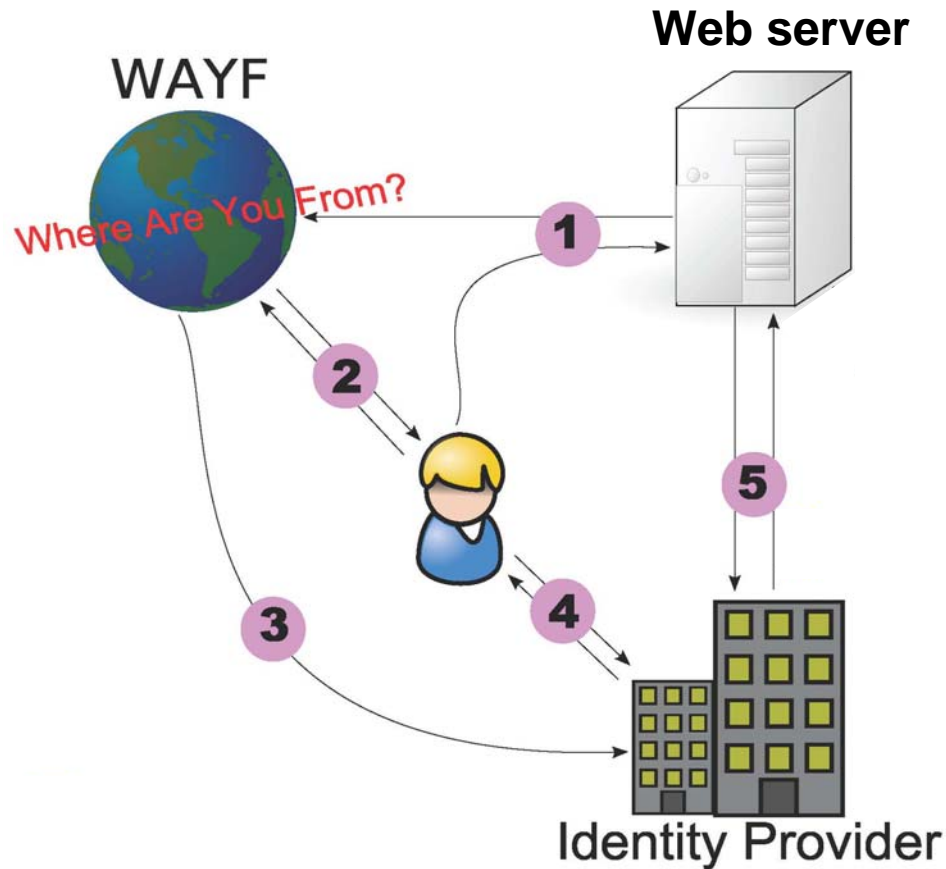


# Shibboleth Overview

- Web-based federated access management system based on SAML
- Based on separation of authentication and authorisation
  - Authentication: Identity Provider (IdP) at user's home institution
  - Authorisation: Service Provider (SP) based on attributes from the IdP
  - Discovery: Where Are You From (WAYF) service
- User can remain anonymous at the SP



# Shibboleth Authentication and Authorisation



(Thanks to Kang Tang)

# ShibGrid Use cases

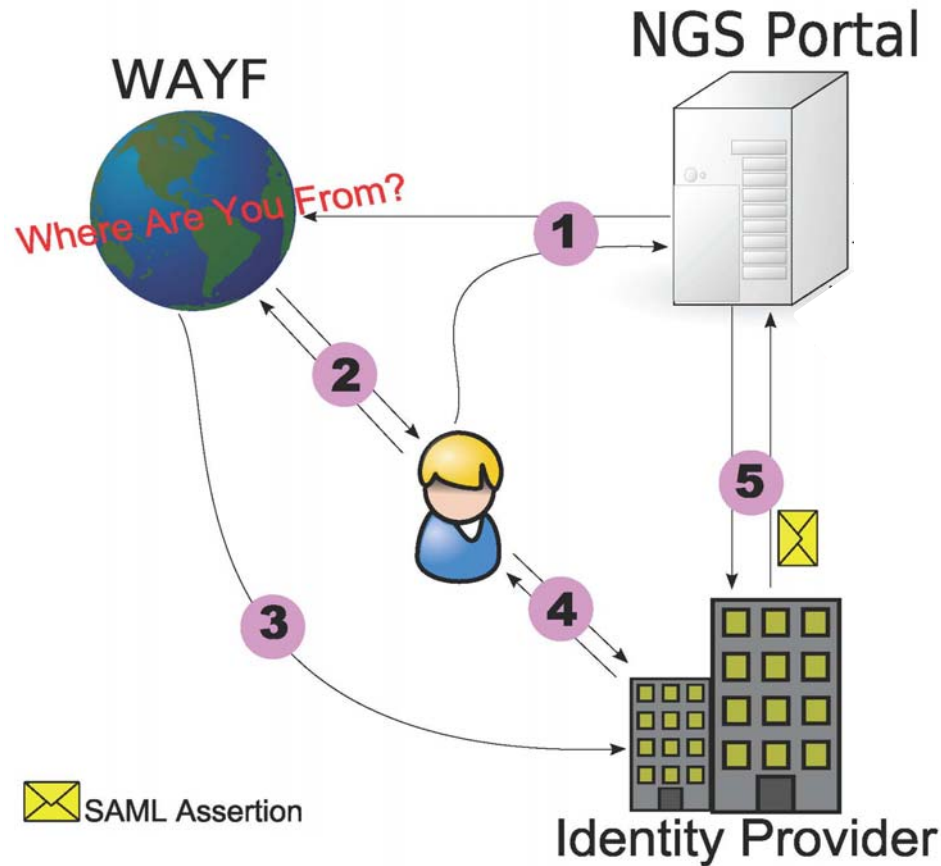
- Allow Access to the Grid solely with Shibboleth
- But use standard Grid certificates when something extra is required – still many advantages
- Access to the Grid through a Portal
  - NGS portal/project portals
- Access to the Grid through other access methods
  - Globus, Java GSI-SSH Terminal, CoG, etc.,
- Registration (for NGS) using Shibboleth



# Architectural Design

- Don't change the user
  - Prevent extra logical steps: portal first
  - Easy to deploy in project portals
  - Support other access methods
- Don't change other services
  - Work within Shibboleth and existing GSI frameworks

# Shibboleth Authentication and Authorisation



(Thanks to Kang Tang)

# More than just portal access...

- Registration service
  - Data Protection Act/Acceptable Use Policy?
  - Link to NGS user registration
- Grid proxy download tool
  - For non portal Grid access methods
- Grid proxy upload tool



# Logon via Shibboleth...

Welcome !

Tuesday, 28 November 2006

The screenshot shows the Stringbeans Enterprise Information Portal NGS Portal. The page has a blue header with the Stringbeans logo and the text "Enterprise Information Portal" and "NGS Portal". Below the header is a "Welcome" section with a blue background. The main content area is white and contains the following text:

This Portal is used for tests by [ShibGrid](#) project.

Existing users can either log in using the form below, or [Login via Shibboleth](#).  
**Note:** You need to [Register your DN](#) before you can login through Shibboleth.

To upload your personal credential into a MyProxy server, use

- [ShibGrid Proxy Upload Applet](#).
- [MyProxy Upload Tool](#)

The "Login" section is enclosed in a blue border and contains the following form:

**User Name:**

**Password:**

Remember my username  
 Remember me

Not Registered?  
[ [Sign up now](#) ]

Forgot your Password?  
[ [Reset Password](#) ]

Forgot your username?  
[ [Request Username](#) ]

# ...Choose your home institution...

Select your home institution

SDSS

Development  
Federation

## Selection options

The service you are trying to reach requires that you authenticate with your home institution. Please select an institution using one of the methods below.

## Recent selections

ShibGrid (CCLRC & Diamond Test Users)

Clear

## Choose from list

AHDS, King's College

Remember for session

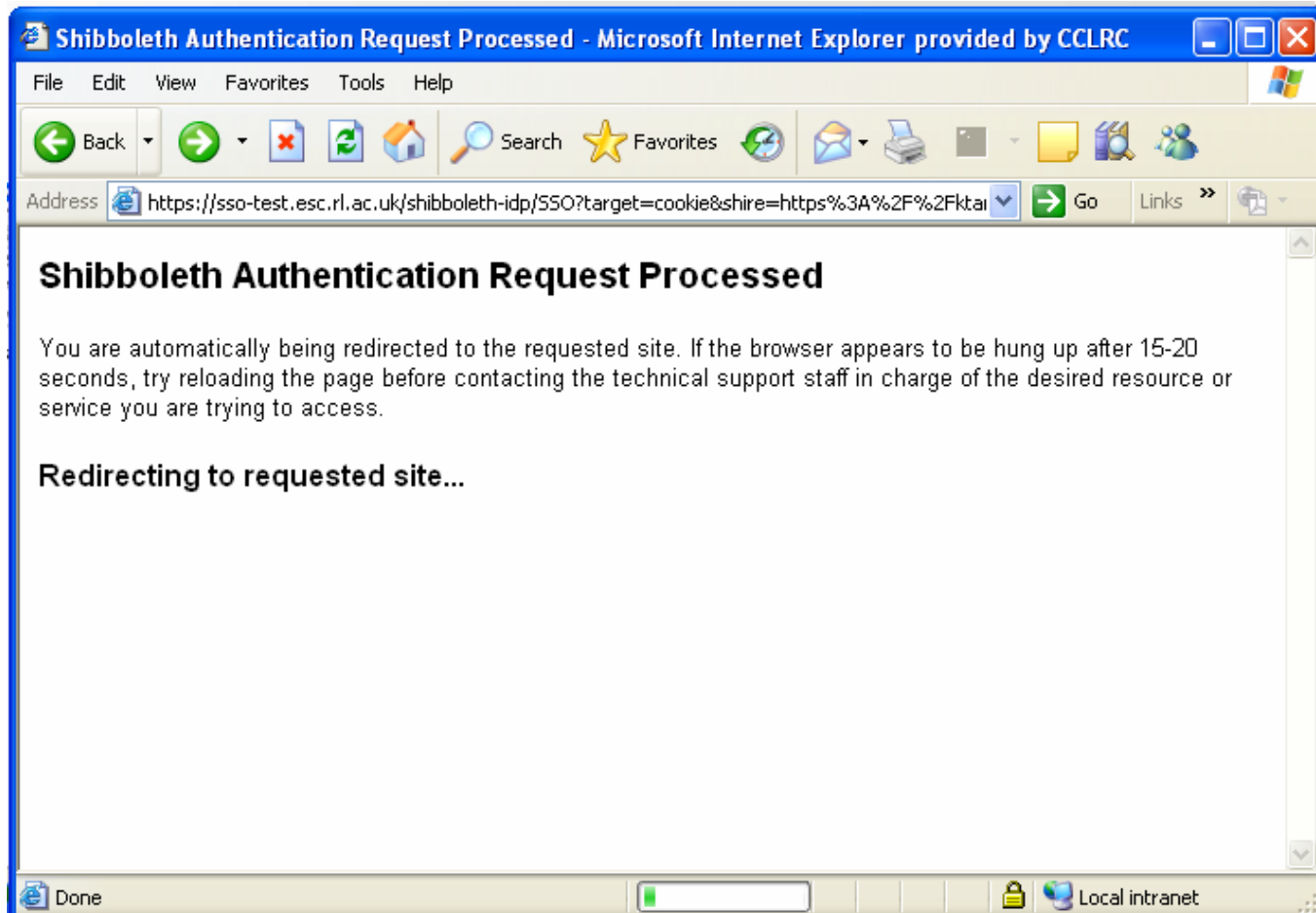
Select

## Search by keyword

Search

Need assistance? Visit the [SDSS Federation web site](#).


...background log-in in using Kerberos...



# ...welcome to the Portal...

Welcome David !

Tuesday, 28 November 2006



Enterprise Information Portal

Preferences | Edit Profile | Sign Off

Home | News | Help | Job Management | File Transfer | SRB Browser | MDS Browser

### Welcome


Congratulations ! You have successfully logged in to Stringbeans Enterprise Information Portal ! Changing your preferred language, color scheme, and default page can be done by clicking the "Preferences" link above. If this is your first time accessing your account, it is highly recommended that you change your password thru the "Edit Profile" link, next to the "Preferences" link above. "Change Password" link can be found on upper right of the "Edit Profile" portlet. You can create a new page, edit or remove an existing page, add or remove portlet(s) from a page thru the icons provided on each page, located at the upper right of the page (icons bar). A list of available portlets can be found when you are modifying (creating or editing) a page.

Thanks for using Stringbeans. We hope it proves to be a fruitful experience. As always, all comments and critiques are welcome and can be conveyed to us by sending us an email to [feedback@nabhinc.com](mailto:feedback@nabhinc.com)

### Search the Internet

Search the web for:

Search engine:

Yahoo 

Search

Powered By [Stringbeans](#)


Copyright © 2005 Nabh Information Systems, Inc. All rights reserved.







# ...and we have an automatically-generated Grid proxy

Welcome David ! Tuesday, 28 November 2006

[Preferences](#) | [Edit Profile](#) | [Sign Off](#)

 Enterprise Information Portal

[Home](#) | [News](#) | [Help](#) | [Job Management](#) | [File Transfer](#) | [SRB Browser](#) | [MDS Browser](#)

Proxy Manager    

### Proxy Manager Portlet

Your available GSI proxy credential is shown below.

<b>Subject:</b>	C=UK,O=eScienceMyProxy,OU=CCLRC,UID=drs65,CN=David Spence,CN=proxy
<b>Issuer:</b>	C=UK,O=eScienceMyProxy,OU=CCLRC,UID=drs65,CN=David Spence
<b>Bits:</b>	512
<b>Time Left:</b>	1 hour(s) 59 minute(s) 56 second(s)

Powered By [Stringbeans](#)

Copyright © 2005 Nabh Information Systems, Inc. All rights reserved.



# DN Mapping in ShibGrid

## Considered:

- `/C=UK /O=eScienceMyProxy /OU=<Institution>/UID=<Site username>/CN=<First name> <Last name>`

Traceable but unworkable with UK Shibboleth Federation

- `/C=UK /O=eScienceMyProxy /L=<IdP entity-id>/CN=<eduPersonTargetedId>`

Not traceable. Non-unique DN across sites.

□

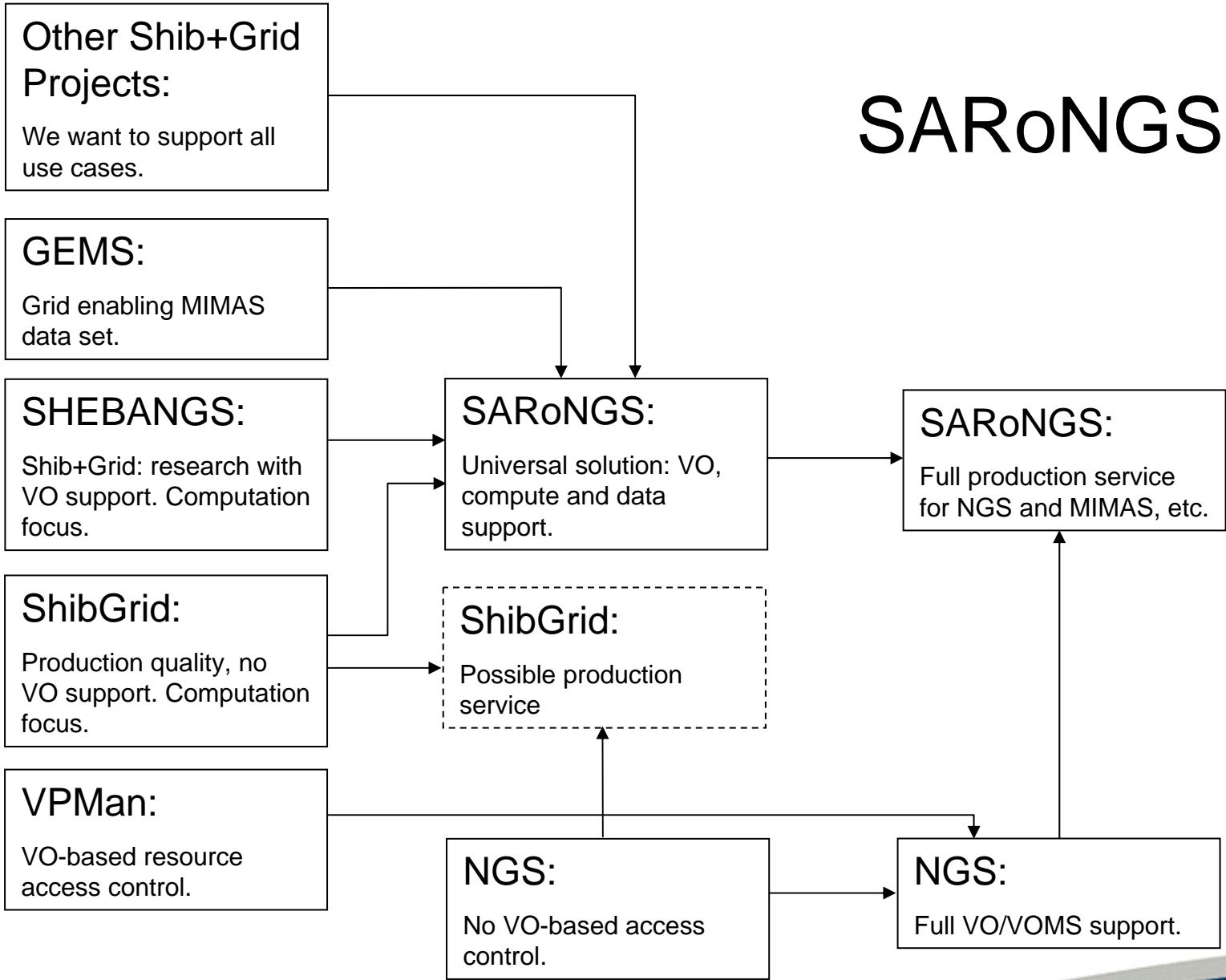
- `/C=UK /O=eScienceMyProxy /CN=<eduPersonPrincipleName>`

Traceable. Recognised UK Shibboleth Federation attribute (but not core attribute). Preferred scheme.

# Other Projects

- “There’s more than one way to skin a cat”
- This list is not exhaustive...
  - UK – SHEBANGS, ShibGrid, GridSite, DyVOSE/VOTES/BRIDGES/GLASS and PERMIS
  - US – GridShib
  - Switzerland – SWITCH (gLite)
  - Australia – MAMS
- SaRoNGS - Shibboleth Access to Resources on the NGS

# SARoNGS



# On-going/Future Work: SARoNGS

- New project starting in January for one year
- Will provide a standard production bridge for all UK Academics from the UK Federation into the Grid world.
- Will combine expertise from ShibGrid, SHEBANGS and MIMAS.
- Will consolidate the various models for Shibboleth and Grid integration into one service.
- Will provide a much simpler model for integrating portals, resources and services.

# Requirements highlights

- User/Project
  - Transparent access to eScience facilities, consistent with other SSO-enabled components.
  - Access to components at home or away (even Internet Café).
  - Fit in with local authentication schemes.
  - Users don't want to know about certificates.
  - Want to use own project portal.
- NGS
  - Must be compatible with:
    - GT2+VOMS and
    - NGS registration system



# Questions

