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...
Choose your home institution...
...background log-in in using Kerberos...
...welcome to the Portal...

Welcome David!

Welcome to the Stringbeans Enterprise Information Portal! You have successfully logged in. Congratulations! 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 through the "Edit Profile" link, next to the "Preferences" link above. The "Change Password" link can be found on the 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 through 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.

Powered by Stringbeans

Copyright @ 2006 Nabh Information Systems, Inc. All rights reserved.
...and we have an automatically-generated Grid proxy
DN Mapping in ShibGrid

Considered:
- /C=UK /O=eScienceMyProxy /OU=<Institution>/UID=<Site username>/CN=<Firstname> <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
SARoSNGS:
Full production service for NGS and MIMAS, etc.

GEMS:
Grid enabling MIMAS data set.

SHEBANGS:
Shib+Grid: research with VO support. Computation focus.

ShibGrid:
Production quality, no VO support. Computation focus.

VPMan:
VO-based resource access control.

NGS:
No VO-based access control.

ShibGrid:
Possible production service

NGS:
Full VO/VOMS support.

SARoSNGS:
Universal solution: VO, compute and data support.

SARoSNGS:
Possible production service for NGS and MIMAS, etc.

Other Shib+Grid Projects:
We want to support all use cases.
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