



# Technopolitical & Technosocial Considerations

## **Great Plains Network A Region-wide VO for Collaboration**

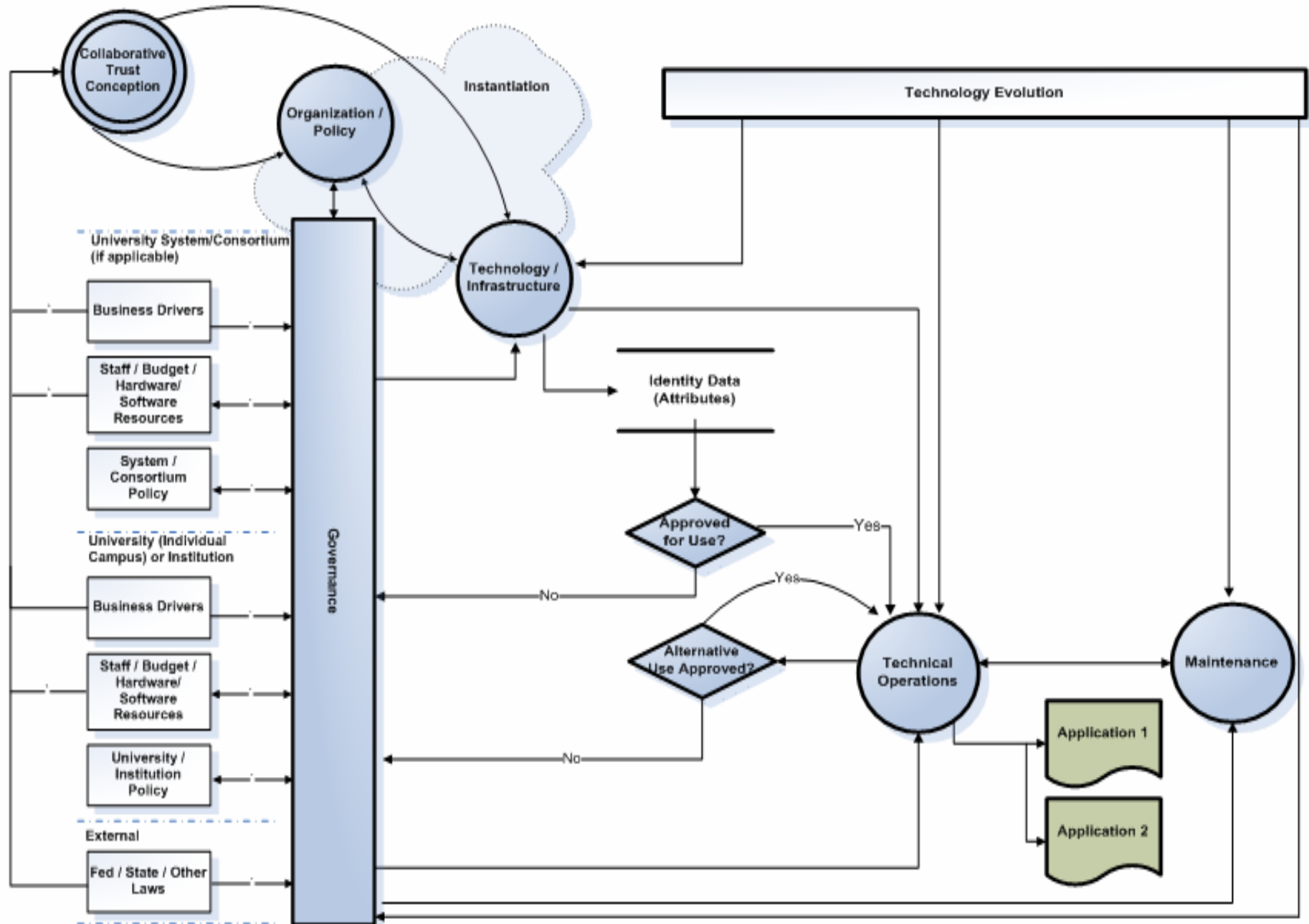
Gordon K. Springer  
University of Missouri - Columbia  
NSF CRCC Workshop  
Arlington, VA.  
April 27, 2006  
(springer@missouri.edu)



# Outline

- IdM Lifecycle Framework for Multi-Institutional VO
- Matrix to address policy & technical issues
- An example using the GPN grid test bed
- Gaps and impediments in existing middleware structures

# Collaborative Identity Management Life-Cycle



From Bright Idea to Concrete Implementation: The Identity Management Life Cycle for Consortia, Educause 2005

<b>Federation</b> (inter-campus)	What data / services shared; <i>Trust Agreements</i>	Multi-campus collaboration or shared access	Privacy-preserving indirection (Shibboleth); security policies	Shibboleth	Certifying Authentication (InQueue) or other agent	Need generic and extensible descriptions
<b>AuthZ service</b> Role- & rule-based access	“allowable” attributes; app needs for data; protect user data		Authorization of roles or groups	MACE Entitlements	Groups; external apps (Signet...)	Reflect business rules in middleware roles, rules
<b>AuthN service</b>			Encrypted traffic;	Authentication	Assistance needed to enable apps	
<b>Web Gateway</b>			SSL; certificates	Dynamically created html	Web interface	
<b>Registry</b>						
<b>Directory</b> ( <i>Reflect</i> )						
	<b>Policies &amp; Stakeholder Interests</b>	<b>Business Case / Marketing / Examples</b>	<b>Security &amp; Privacy</b>	<b>Technology</b>	<b>Deployment strategies</b>	<b>Integration</b>

**From Bright Idea to Concrete Implementation: The Identity Management Life Cycle for Consortia**



# The Great Plains Network (GPN)

## Region-Wide Collaboration Environment





# Background

- 7 States in region (AR, KS, MO, ND, NE, OK, SD)
- GPN connected all states to Internet2/Abilene network as a gigapop. 3 states now connected and 4 are collaborating partners
- GPN has a history of network infrastructure collaboration - Midnet (1987) then GPN (1997)
- **Can this history be turned into a collaborative research and education environment using middleware?**

# Project Basis

- Using **Shibboleth** for inter-institutional authentication for collaboration in a VO
- Using **MACE** Entitlements for fine-grained authorization to access specific resources
- Enabling access to **grid**-based resources
- Deploying applications to demonstrate the integration in action

# Progress to Date

- Strategic planning on a regional basis to deploy Shibboleth authentication for collaborative activities including grid-based applications
- Campus middleware assessment on campuses to determine impediments to moving forward
- Build a middleware test bed on two campuses to demonstrate interoperability for limited applications (now being deployed at 4 sites)
- Attend and conduct workshops focused on middleware deployment (e.g., Shibboleth, Grid)

# Challenges

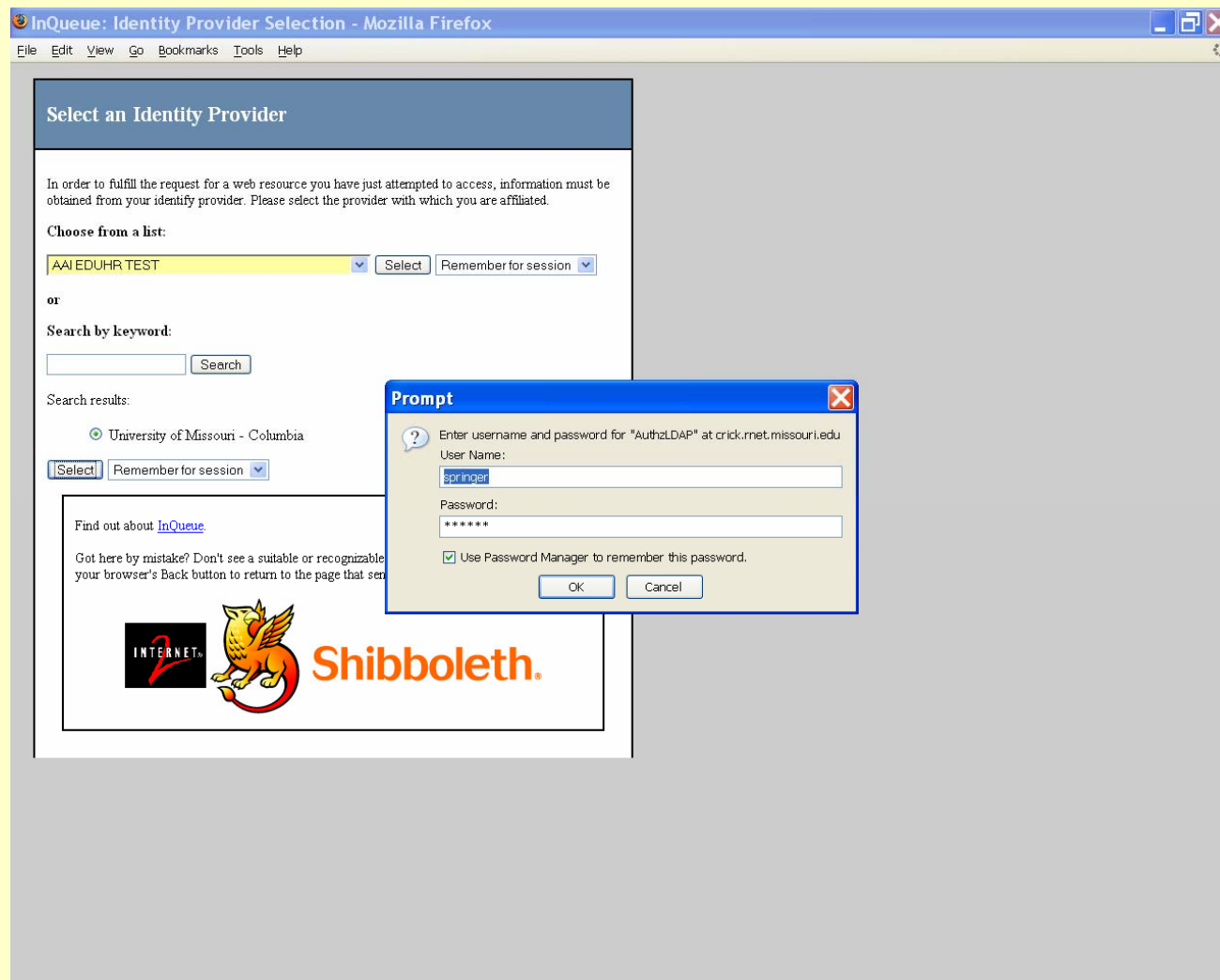
- Dealing with policy issues among multiple institutions
- Defining entitlements for coarse-grained and fine-grained authorizations under control of VO
- Developing a strategy for authorizing and managing entitlements with standardized tools (e.g., Signet and Grouper) in a federation
- **Moving a test bed environment toward a production level environment with a broader scope to support regional research and education activities**



# Grid Computing at MU & UARK & ...

- Have two grid computing resources from which to choose
- MU grid focused on data repository and BioSci applications
- UARK grid focused on MPI program development and execution
- **Now ... adding 3 clusters donated by Sun to GPN to develop shared GPN Grid resources located at KU, MU, NU and UARK to enable distributed grid deployment with multiple services in a VO, which is independent of any particular institution.**

# A Quick Tour ... Authenticating at Crick



The screenshot shows a Mozilla Firefox browser window titled "InQueue: Identity Provider Selection - Mozilla Firefox". The main content area is titled "Select an Identity Provider" and contains the following text: "In order to fulfill the request for a web resource you have just attempted to access, information must be obtained from your identify provider. Please select the provider with which you are affiliated." Below this, there is a "Choose from a list:" section with a dropdown menu showing "AAIEDUHR TEST" and a "Select" button. An "or" separator follows, then a "Search by keyword:" section with a search input field and a "Search" button. Under "Search results:", there is a radio button selected for "University of Missouri - Columbia" and a "Select" button. At the bottom of the main content area, there is a link "Find out about InQueue" and a message: "Got here by mistake? Don't see a suitable or recognizable your browser's Back button to return to the page that ser".

Overlaid on the main content is a "Prompt" dialog box with the following text: "Enter username and password for 'AuthzLDAP' at crick.net.missouri.edu". It contains two input fields: "User Name:" with the text "springer" and "Password:" with "\*\*\*\*\*". There is a checked checkbox for "Use Password Manager to remember this password." and "OK" and "Cancel" buttons at the bottom.

At the bottom of the main content area, there is a logo for "Shibboleth" featuring a phoenix and the text "INTERNET. Shibboleth."



# Shib Target - on Crick

GP.Middleware Shibboleth Repository - Project Access - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://crick.rnet.missouri.edu/GPN/

**GP.Middleware Shibboleth Repository**

[Access to Site Data](#)

[Project Access](#)

**Participants**

[GPN-ETR Presentations](#)

Done crick.rnet.missouri.edu Disabled



# GPN MACE Entitlements

GP.Middleware MACE Documentation - GreatPlains.Net - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.greatplains.net/mace-gpn/

**GP.Middleware MACE Documentation Site**

**MACE Documentation for Greatplains.Net Namespace and Entitlements**

MACE (the Middleware Architecture Committee for Education) has delegated the operations of the Uniform Resource Name (URN) namespace `urn:mace:greatplains.net` to the [Great Plains Network](#).

This namespace supports the assignment of unique, global, persistent names to resources used by the Great Plains Network in its Shibboleth and other middleware initiatives.

For more information about URNs, see:

- Internet2/MACE Uniform Resource Name (URN) registry [home page](#).
- [RFC 3613](#), which defines the urn:mace namespace and describes the procedures and policies governing its use.

**Namespace & Entitlements Administered by the Great Plains Network**

Namespace	Purpose	Date registered	Registry URL
urn:mace:greatplains.net	Enterprise Namespace	2005-03-31	<a href="#">Enterprise</a>
urn:mace:greatplains.net:biosci	BioSci Entitlement	2005-05-12	<a href="#">BioSci</a>
urn:mace:greatplains.net:biogrid	BioGrid Entitlement	2005-05-12	<a href="#">BioGrid</a>
urn:mace:greatplains.net:repository	Data Repository Entitlement	2005-03-31	<a href="#">Repository</a>
urn:mace:greatplains.net:uark.edu:webmpi	Web MPI Entitlement	2005-04-25	<a href="#">WebMPI</a>

Questions about registrations under urn:mace:greatplains.net, including suggestions for new registrations, should be directed to the [Authentication & Authorization Services Team](#).



For other information and queries, please contact: [GPN MACE Administrator](#).

Done Disabled



# Main Menu

https://genome.rnet.missouri.edu - Menu Options - Mozilla Firefox

 **GP.Middleware Shibboleth Repository** 

## Menu Options

---

User: [springer@missouri.edu](mailto:springer@missouri.edu) Login Time: Wed Apr 19 21:23:39 2006

### Menu Options

- File Process
- File Upload
- [GO](#) MU Swine Genomics Project
- [GO](#) WebMPI - University of Arkansas
- [GO](#) Biotools

[Print This Page](#)

---

Page Generated Wed Apr 19 21:23:39 2006.  
Please send comments to: [wwwadm@rnet.missouri.edu](mailto:wwwadm@rnet.missouri.edu)

Done genome.rnet.missouri.edu Disabled





# Grid Computing at MU

A screenshot of a Mozilla Firefox browser window. The address bar shows the URL 'https://genome.rnet.missouri.edu - GPN BioSci - Mozilla Firefox'. The page content includes the GPN logo, the title 'GPN BioSci - Bioinformatic Tools' with the MU logo, and a section titled 'Please select one of the following analysis tools:'. Below this title are three buttons: 'WWWBlast' with the text 'Run the Web Version of the Blast Tool', 'MPIBlast' with 'Run the MPI Version of the Blast Tool', and 'Clustal' with 'Run the Clustalw Utility'. A 'Print This Page' link is also present. At the bottom of the page, it says 'Page Generated Sun Feb 12 10:21:46 2006' and 'Please send comments to: [wwwadm@rnet.missouri.edu](mailto:wwwadm@rnet.missouri.edu)'. The browser's status bar at the bottom shows 'Done', the address 'genome.rnet.missouri.edu', and a 'Disabled' indicator.



# Grid Computing at UARK

https://genome.rnet.missouri.edu - Menu Options - Mozilla Firefox

 **GP.Middleware Shibboleth Repository** 

**Menu Options**

---

User: [springer@missouri.edu](mailto:springer@missouri.edu) Login Time: Wed Apr 19 21:23:39 2006

**Menu Options**

- File Process
- File Upload
- [GO](#) MU Swine Genomics Project
- [GO](#) WebMPI - University of Arkansas
- [GO](#) Biotools

[Print This Page](#)

---

Page Generated Wed Apr 19 21:23:39 2006.  
Please send comments to: [wwwadm@rnet.missouri.edu](mailto:wwwadm@rnet.missouri.edu)

Done genome.rnet.missouri.edu Disabled



# UARK WebMPI Target

The screenshot shows a web browser window with the address bar displaying `http://webmpi.csce.uark.edu - Web-MPI Webservice tools - Mozilla Firefox`. The main content area is titled "Web-MPI Cluster Webservice tools" and contains three underlined links: [Target Server environment test](#), [Shibboleth environment test](#), and [MPI Web-service test:](#). Below the links are two logos: "POWERED BY Mac OS X" and "Powered by APACHE".

**Note: we got here by passing Shib credentials obtained to authenticate at MU SP site to UARK and the entitlements of the requestor included WebMPI, which was accepted by the UARK SP based on a trust relationship with MU SP. No separate authentication was required for access.**



# Ready to Compute

A screenshot of a web browser window showing the MPI Webservice interface. The browser's address bar displays 'http://webmpi.csce.uark.edu - MPI Webservice - Mozilla Firefox'. The page title is 'MPI Webservice'. Below the title is a navigation menu with tabs for 'Start', 'Upload', 'Compile', 'Execute', and 'Results'. The main content area is titled 'MPI Web Interface to the Hawk Cluster' and lists the steps for executing an MPI program: 1. Upload an MPI program source file, 2. Compile an MPI program source file, 3. Execute an MPI program, and 4. View Execution Results for the MPI program. Below this is a section for 'Hawk Cluster Configuration' with details: 'Compute Nodes: 4 - Dual Opteron 242 - 1600 Mhz', 'Memory per node: 2 Gb', and 'Interconnection: Gigabit Ethernet'. A section for 'MPI programming guide and References' includes links to 'The Message Passing Interface (MPI) standard', 'MPI Routines', and 'MPI Tutorial'. At the bottom, a paragraph states that the project is supported in part by the GPN Extending the Reach project, with funding from Educause on behalf of the NMI-EDIT Consortium of Internet2, Educause, and SURF, and with several statewide university systems and regional networks. For more information on GPN ETR, it refers to the GPN home page.

# Open Problems

- Administering eduPerson entitlements using common, secure, and authorized tools among the VO institutions (that conform to institutional policies) ... plus those of GridShib, Signet, Grouper, Globus, OSG, CABig, IRBs, ...
- There are almost as many CA authorities as there are users ... and trust relationships among them are mostly non-existent.
- Identifying and refining the entitlements for hierarchical and peer relationships are out of the hands of the VO itself. The entitlements must be independent of IdP.

# Open Problems (cont.)

- Differing institutional policies makes it difficult to get everyone on the same page. Some institutions don't have an institutional IdP or a compatible one that can be used in this environment.
- Collaboration is between and among individuals, but encouraging their involvement is difficult in such a diverse environment when they don't have any input/control in the process to let them collaborate .
- Individuals not part of some institution cannot participate without special action by VO and some participating institution.



# What is the Pay Off ? Success or Failure?



**Questions ?**