



Great Plains Network Consortium

Great Plains Network: Building the Regional Middleware Infrastructure

NMI-EDIT Case Study Series

In response to calls from the higher-education community, the NMI-EDIT Consortium has developed a series of Identity Management Case Studies to explore the planning and implementation of this critical infrastructure at higher-education institutions around the country.

In the spring of 2004, NMI-EDIT released the Extending the Reach Call for Proposal with the overall vision of exploring possible models for middleware support and informing the NMI-EDIT outreach and development efforts through collaboration with a wider, more diverse group of institutions. The work outlined in this case study was supported in part by the NMI-EDIT Extending the Reach Program.

This NMI-EDIT Case Study Series is sponsored by the National Science Foundation Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium of EDUCAUSE, Internet2, and SURA. Additional support was provided by the National Science Foundation Cooperative Agreement NSF 02-028, ANI-0123937. Thanks are extended to authors Amy Apon, Greg Monaco, Gordon Springer, and Kathryn Huxtable.

Copyright © 2006 by the University of Arkansas and the Great Plains Network Consortium. The University of Arkansas and the Great Plains Network Consortium permit use of the content for noncommercial purposes with attribution. All rights reserved.



Executive Summary

The Great Plains Network (GPN) is a regional consortium of public universities in the states of Arkansas, Kansas, Missouri, Nebraska, Oklahoma, North Dakota, and South Dakota. Its partners include its predecessor, MIDnet. The long-term goal of GPN was and continues to be to build a regional networking and middleware infrastructure to share resources among the participants. In June 2004, GPN was selected to be one of four projects in the Extending the Reach (ETR) program funded by the National Science Foundation Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium¹.

The goals of the GPN ETR project are to:

- 1) Develop a region-wide collaboration environment through the development of middleware services,
- 2) Build a regional middleware infrastructure for sharing resources, and
- 3) Engage in strategic planning on a regional basis.

Challenges to meeting these goals include the geographic distance between participants, lack of central authority, and heterogeneous approaches to these problems on the multiple campuses involved in the project.

The results of this project include a working test bed that is accessible by GPN participants. The test bed includes prototype applications in the areas of file and data

sharing, shared use of a cluster computing computational resource, and shared access to three applications in the area of biological sciences. The Shibboleth architecture for web-based authentication and access control and several other key NMI-EDIT middleware components are incorporated into the test bed.

This case study describes the challenges encountered and lessons learned in building the GPN virtual organization. The GPN has found that collaboration among individuals is essential, that the middleware effort will be limited by the level of the support of the participating institutions, and that it is essential to remain aware of current events and changes within the broader middleware community. The GPN's middleware infrastructure building is an on-going effort. The next goal for the GPN regional middleware infrastructure is to move towards a production quality set of tools in support of research and education in the region.

More information about this GPN ETR Case Study is available at the GPN ETR web site² and also by contacting Amy Apon at aapon@uark.edu.



¹ <http://www.nmi-edit.org/index.cfm>

² <http://archie.csce.uark.edu/gpn/H>

NMI-EDIT Components Highlighted in this Case Study

eduPerson Directory Schema

<http://www.educause.edu/eduperson>

eduPerson contains identity-related attributes for higher-education institutions to deploy to foster inter-institutional collaborations.

Shibboleth System

<http://shibboleth.internet2.edu>

The Shibboleth System support inter-institutional sharing of web resources that are subject to access controls.



Great Plains Network: Building the Regional Middleware Infrastructure

The Great Plains Network (GPN) is a regional consortium of public universities in the states of Arkansas, Kansas, Missouri, Nebraska, Oklahoma, North Dakota, and South Dakota and regional higher-education state networks in these states. Its partners include its predecessor, MIDnet. In 1997, funded by the National Science Foundation (NSF), the GPN Consortium constructed a high-speed network to support the earth system science community among member universities. That network interconnected member universities and then connected them to the greater Internet2 community via the Abilene network and, via Abilene, to high-speed networks on other continents.

Since it was built, the GPN has undergone several dramatic changes in focus, in part because by 2001, three of the initial seven connected states were now connecting elsewhere and their interest in GPN was no longer physical infrastructure but rather collaborative research opportunities. Between 2003 and 2005, GPN was struggling to re-invent itself to provide its university constituency not only with networking infrastructure and with technical and non-technical support services, but with research and educational leadership as well .

In the winter of 2003 - 2004, while in the process of polling the membership on

technical training needs, the topic of middleware received nearly unanimous support. Member representatives were polled in person and by email on their interest in a regional middleware project. The vast majority of the responses were highly favorable and included comments such as:

- “I like that idea and see much benefit in our smaller states. How can we help?”
- I have wanted to participate in such an initiative for quite some time, only there are just so many hours in a day.
- I think this is a great effort and it will be very helpful for all schools.”

By the spring 2004, Internet2 member meeting, campus representatives were strongly in favor of partnering to develop middleware expertise across campuses in the region. The member representatives recognized the strategic importance of sharing resources collaboratively and shared the goals of national efforts devoted to facilitating inter-institutional collaboration, such as the NMI (NSF Middleware Initiative)), NMI-EDIT (NSF Middleware Initiative - Enterprise Desktop and Integration Technologies) and Shibboleth³. By early April of 2004, there was commitment across eleven campuses to seek funding for a GPN middleware

³<http://shibboleth.internet2.edu/H>



project. The long-term goal was and continues to be to build a regional middleware infrastructure to share resources across the region. Nine of over twenty-three campuses served by GPN and MIDnet have participated in the project, including the University of Arkansas, University of Kansas, University of Missouri-Columbia, University of Nebraska-Lincoln, University of Oklahoma, North Dakota State University, the Peter Kiewit Institute (University of Nebraska at Lincoln and Omaha), University of South Dakota, and South Dakota State University. The project has support from all state networks.

Business Challenge

While national networking and networking-related initiatives such as the NMI present new opportunities to improve network capacity, security and reliability for research activities, these initiatives also present challenges to the GPN region campuses that are spread across the central United States. Physically separated from one another by long distances and from major research concentrations on the East and West Coast, networking infrastructure development presents a unique opportunity for GPN campuses to peer with one another and their coastal counterparts, provided that the GPN region campuses do not fall behind as new developments unfold.

In addition to geographic challenges, the GPN faces a number of additional hurdles in the deployment of a regional middleware

infrastructure, including the lack of a hierarchical organization or a single central authority, and heterogeneous approaches to the implementation of core middleware services across its campuses.

Lack of Central Authority

The GPN consortium is a regional membership organization that has public university campuses in seven states as its participants. Campuses in five of the seven states belong to state networks (see Appendix A) and these networks may be legislated to represent all public K-20 schools, libraries and hospitals within their state. GPN is best able to influence regional decision making by calling attention to best practices. This has historically been done through GPN Annual Meetings and regional technical workshops in key areas such as IPv6, multicast, security, and wireless networking.

Heterogeneous Approaches to Middleware Deployment

At the inception of this project, the proposed participants were at varying stages of planning and implementation for core middleware services, including the Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory® systems, and even locally-developed identification and authorization systems. Middleware deployment at the participating campuses, a brief history of the regional and state organizations, and a complete list of the campuses to be served via strategic planning and workshop activities are included in Appendix B.



Solution

History of Collaboration

In spite of heterogeneous organization and lack of central authority, the campuses and state networks within the GPN region have twice used collaborative strategies in the area of networking and infrastructure to create win-win situations for all. The first collaboration was the formation of MIDnet in 1987, followed by the formation of GPN itself, 10 years later. These community solutions typically provided the region with the critical mass necessary to achieve economies of scale, coordinated planning, and consequent cost reduction.

In one sense, this middleware project is an attempt to see whether the success of peer collaborations, when focused on cost-reduction in the purchase or lease of infrastructure, can successfully be extended to an infrastructure-related project with a different set of priorities, namely human capacity-building, training and consulting, and shared resources across campuses and state networks.

As an organized GPN approach to regional middleware infrastructure began to unfold in early 2004, an active community of interest was developed through weekly teleconferences and a mailing list that initially included eighteen participants from the nine participating campuses. A significant characteristic of this community is that it includes a voluntary collaboration of both academic computing personnel and

researchers. This community developed the proposal to the NMI-EDIT ETR project.

Project Goals

To accomplish the goals of standardization and interoperability, the first year short-term goals for this project included:

- Strategic planning on a regional basis
- Implementation activities on two campuses
- Campus middleware assessment activities
- Interoperability testing of various middleware tools
- Direct consultation
- Two regional middleware workshops
- Educational outreach

The project has ongoing goals that include:

- Continuing the work of the strategic planning committee with outreach to virtual organizations (VOs) across campuses (including supercomputing resources)
- Undertaking additional implementations across campuses and VOs
- Continuing regional middleware workshops and educational outreach both within and beyond the region

The broader project objective was to leverage resources to expand middleware capabilities across the diverse group of campuses and state networks in the GPN/MIDnet region with the potential of, ultimately, impacting libraries, hospitals and other entities in the region. The strategic plan and campus implementation case studies will be broadly available beyond the region. The project will ultimately extend



the reach to campuses beyond the high performance networking community, including campuses that have not begun the process of implementing core middleware services. Ultimately, the project intends to serve as a model for moving groups of institutions into a position of active collaboration based on regional interests. The model should prevent institutions from having to “do it alone.”

In order to maximize the impact of this project, appropriate higher education state networking organizations were engaged in the development and support of this project. State networks set policy and standards, connect higher education, K-12, state libraries and often provide Internet access to state government. Including these entities greatly extends the reach and impact of project activities.

Project Plan

- The objectives of the project plan are to:
 - Develop a knowledge base, including the test bed installation and testing of middleware environments
- Provide educational outreach
- Develop deliverables

The timeline for Year 1 of the project is shown in Table 1 in Appendix C.

Development of a Strategic Planning Committee

The first and, perhaps, most important component of the plan is to have a strategic planning committee, with widespread representation, to guide and contribute to the development of the GPN middleware effort

over the next two years. The Strategic Planning Committee has evolved from the initial community of interest that developed the proposal to NMI-EDIT. This group, which is largely composed of volunteers, includes members of institutions within GPN that are faculty, researchers, information technology staff, and technology administrators. It is responsible for setting goals and evaluating progress.

Development of a Knowledge Base/Human Knowledge Network

During the first year of the project several steps were identified for building a knowledge base:

- Identify existing regional expertise.
- Increase regional expertise.
- Establish a middleware testbed that can be used to test installation procedures and interoperability of middleware environments.
- Identify and publicize the availability of regional consulting expertise.

Arising from the biweekly teleconferences that led to the proposal to NMI-EDIT, individuals with unique expertise in middleware and Shibboleth, in particular, were identified. Because of the strong encouragement from the funding agency to include the Shibboleth architecture as a key component of the middleware test bed, the GPN saw a need to increase regional expertise in this area.



Educational Outreach

Members of the project meet biweekly via phone and Access Grid technology. Many of the initial meetings involved presentations by regional experts. The meetings have also been used to bring in expertise from outside the region to update members on current trends and innovations (e.g., InCommon, Grouper, Signet). Contact and sharing of information between members at different institutions has also been facilitated by an email list.

In the summer and fall of 2004, members of the GPN project attended Shibboleth workshops and Install Fests sponsored by NMI-EDIT and the GPN group itself. More than a dozen members from GPN institutions, representing at least eight campuses, attended the Camp Shibboleth sponsored by NMI-EDIT during June 2004. Several of the members also attended an Install Fest that was held in conjunction with the Camp. In the summer of 2005 the project supported the annual Great Plains Network and sponsored faculty and graduate student travel to the meeting to hear from regional and national experts in middleware and grid computing. Approximately 120 people representing all GPN states attended the meeting, making this the largest meeting ever held by GPN. Many faculty and students also presented their efforts at a poster session at the meeting. A one-day workshop on Globus Toolkit 4 was also held and was attended by over twenty participants.

Additional Deliverables

A Middleware Survey was developed by a subset of the project team, to measure, with respect to middleware, in general, and Shibboleth, in particular, the status at each campus of any middleware implementation and broader goals for middleware. Due to attendance at Camp Shibboleth and various Shibboleth Install Fests, followed with Shibboleth implementation at multiple participating campuses, the participating GPN campuses had not only already begun implementing middleware components on their campuses, they had quickly surpassed the level of implementation being queried in the survey questionnaire and were moving in more advanced directions.

Middleware Test Bed Components

Encouraged by the funding of their ETR Proposal in June, 2004, the GPN began their middleware deployment that would support resource sharing among members of the GPN institutions by developing a test bed that included:

- Shibboleth
- Integration with campus identity management systems
- The development of prototype resources
- Creating a namespace and attribute architecture



Shibboleth Base Software

NMI-EDIT's Shibboleth is a project and software package from MACE⁴. It is a protocol and architecture for sharing attributes among trusted institutions, and is designed to authorize a user to a remote web-based resource through the use of the login and attribute information that is maintained at the user's home institution. Shibboleth allows user privacy to be maintained and can also be used to enforce levels of access based on user characteristics

Overview of Software Components

Shibboleth¹ consists of two primary software components. The **Identity Provider (IdP)** component of Shibboleth is integrated with the identity management system of a user's home institution. It authenticates a user using local authentication mechanisms, and then allows user attribute information that is maintained in an institutional identity directory to be sent to a requesting remote resource. The **Shibboleth Resource Provider (RP)** software component protects access to a resource from remote users, allowing them access only if they meet the resource's attribute requirements.

Shibboleth strongly relies on the software servers and protocols that form a trust relationship for passing user authentication and attribute information between the user's home institution (the IdP) and the institution that provides the resource (the RP). The provider components must both own a public key certificate that is signed by a common

Certificate Authority. In addition, the providers must also both be configured to accept requests from the other institution. For resource access to be granted to the user, the IdP must accept requests from the RP to release needed user attribute information. The RP must be configured to allow access by users from the IdP institutions that hold appropriate attributes.

Installation and Training Issues

One of the first goals in the ETR project was to educate the GPN community about Shibboleth and to begin to understand the issues that would be faced when integrating Shibboleth with local identity management systems. In addition to the participation in Camp Shibboleth in June of 2004, members from the University of Missouri also attended a follow-on Shibboleth Install and Config held at the Internet2 Member Meeting in September 2004. Following these two events, GPN members themselves led a workshop talk and a third Install Fest in conjunction with the Oklahoma Supercomputing Symposium in October of 2004. This Install Fest had participants from six teams from GPN. The goal in each of the Install Fests was to build and configure a working Shibboleth IdP system at the member's home institution.

Not all participants in the Install Fests came away from the event with a working IdP. However, the momentum that was gained by these events was significant, and, also significantly, experts within GPN on the various technologies began to emerge. By

⁴ Internet2's Middleware Architecture Committee for Education: [Hhttp://middleware.internet2.edu/MACE/H](http://middleware.internet2.edu/MACE/H)



spring, 2005, seven of the participating institutions had a working IdP.

Campus Directory Integration

Integrating Shibboleth with local campus directory and identity management systems is one of the challenges faced by GPN participating campuses. This task has been complicated by the heterogeneous approach to identity management on the various GPN campuses. In general, campuses that have an LDAP-based identity management system and who were successful at building a preliminary installation of a Shibboleth IdP were successful in their integration efforts during the first year of the project. This integration process is relatively well understood and there are experts within the Shibboleth community that are available to help. In contrast, none of the campuses with a Window's Active Directory system or another non-LDAP-based identity management system were successful with this integration during the project's first year. This may be partly due to the lack of support within the GPN community for these types of Shibboleth integrations.

Support for Federating

The InCommon⁵ federation is operated by Internet2 to support research and education among institutions of higher education. InCommon is built using the Shibboleth architecture. GPN institutions that participated in the early Install Fests joined InQueue⁶, a test federation organized by Internet2 for

institutions that are learning how to use Shibboleth and the federated trust model

A formal federation organization supports the GPN federation process in two ways. First, GPN members of InQueue initially configured their IdP with a public key certificate from the Bossie Certificate Authority recommended by InQueue, since this was easy and at no cost. The Bossie CA is not secure or suitable for production use, but does provide a simple and fast way to build a working prototype Shibboleth system. As GPN members have moved toward production use of their IdP, the Bossie certificates have been replaced by certificates from Verisign and other production-quality CA's to support Shibboleth applications in local campuses. InCommon is a formal federation that has been developed to support a production CA and production use of the Shibboleth architecture across institutions. In general, in order for the identity and RPs in GPN to continue to trust each other, they have to be configured with the public key of each CA that is in use and is trusted in a production setting by the GPN members. InCommon provides a single CA that all member institutions can trust. At the time of this Case Study, most GPN institutions are not members of InCommon, although many are considering joining.

A second way that a formal federation organization supports the GPN consortium is by supporting a WAYF, or a "Where Are You From?" server. In the Shibboleth protocol, when a user first contacts a RP through a web

⁵ InCommon: [Hhttp://www.incommonfederation.org/H](http://www.incommonfederation.org/H)

⁶ InQueue: [Hhttp://inqueue.internet2.edu/H](http://inqueue.internet2.edu/H)



page, the RP must determine the home institution of the user for that person to be authenticated. The Shibboleth protocol redirects a request to the WAYF named by the RP. The WAYF, in turn, maintains a list of potential IdPs, allows the user to select one, and then redirects the user to the authentication process of the IdP selected by the user.

InQueue's WAYF currently supports dozens of participating organizations, which was distracting during testing with GPN resources. In addition, the InQueue WAYF does not meet GPN's needs for the testing and configuration of the middleware test bed. As attributes are being tested, for example, two IdPs have been maintained at the University of Arkansas. The first remained integrated with the campus Identity Management system and was visible to all campus users, but the second was configured in a test mode to only allow access by certain test user accounts. GPN has built a test federation by implementing a test WAYF that lists the test IdP. In turn, the resources also being tested are configured to redirect users to the test WAYF. This lightweight test environment provides a mechanism for introducing new resources and new types of attribute access without interfering with the possible production use of Shibboleth on some campuses. As the middleware infrastructure of GPN grows the components in the lightweight test environment will be replaced by production versions of these components.

Prototype Resources

As early as fall, 2004, participants in GPN/ETR were looking for a business reason to dedicate continuing resources to the project. Although participants were eager to federate, and several simple prototype RPs had been implemented, none of these prototypes provided a real service that required remote user authentication and authorization. The need for the identification and development of a set of real Shibboleth resources became apparent.

GPN Repository

The GPN Repository is a data storage facility that permits members of the collaborating institutions to store and retrieve documents, data and other materials that are to be shared among all of the members. The GPN repository became available to users during the fall of 2004. Access to the GPN repository is protected by Shibboleth and user authentication to a GPN institution. Currently, access is provided to the GPN repository to any user who is a member of a GPN ETR institution.

Offering the GPN Repository is motivated by the need to share large documents within the GPN. Frequently, and many times inappropriately, email (with attachments) is used to share materials among various groups of people. Some of these materials may be quite large and cause many problems such as overflowing mailboxes, unnecessary data duplication, and can easily become outdated for time-sensitive materials. In general, email is quite inefficient in utilizing resources among



collaborators. The GPN repository attempts to overcome some of these inefficiencies by having the materials collected, organized and accessible in one (or more) locations, with access restricted to the members of the GPN federation and without a lot of administrative overhead. While the repository presently is used to house documents, presentations and other GPN/ETR materials, in the longer term the repository can also be used to provide high performance access to data used by application programs in grid computing environments among the VO group servers at several institutions.

An ongoing and complementary project is the development of a web-based Subversion⁷ document repository system that is also protected by Shibboleth. Subversion allows document check out and check in, and will allow the protection of document subdirectories based on user attributes. The Subversion system is expected to be made available to GPN members in fall, 2005.

Biomedical Application

In order to demonstrate the use of entitlements within the defined framework, a working research application in animal genomics was converted from its original user interface that required a Java applet to authenticate and authorize access to the research data by members of the research team. Using the Java applet along with a security database identifying users to be granted secure access to the data, members

of the research team could access the data via a standard web browser. No access to the web site or the data is allowed except to the researchers. The user interface was custom designed and implemented for the protection of this data for the research team.

To make this application available via Shibboleth, the only change required was to replace the existing Java applet front-end with a link on our Shibboleth target application web page to the original application's main web page. This link makes a call to a customized "Shiblogin" command that internally logs the requesting GPN Shibboleth-authenticated user into the protected genomics web site. This is accomplished without the user having to provide a separate login id and password to the application.

The "Shiblogin" command receives the Shibboleth generated credentials and eduPersonEntitlements that are verified, in the login process, to ensure that the credentials provided are from an active Shibboleth session and that the required MACE entitlements from the user's eduPersonEntitlements authorize the user to access the genomic data. No changes to the original application were required and only one additional userid and password had to be added to the application's security database to grant access to the application by all GPN/ETR VO members with the BioSci MACE entitlement.

Within the genomic application, all of the

⁷ Subversion: [Hhttp://subversion.tigris.org/H](http://subversion.tigris.org/H)



Shibboleth credentials as well as the application's "Shiblogin" information, is available for the application to use, as needed, in order to provide even more fine-grained control of access (for example, GPN/ETR users cannot change any data since they have read-only access to all of the research data.)⁸

WebMPI

WebMPI is a Shibboleth application that enables remote users to access a Linux cluster, via a web browser, in order to run parallel applications. A typical user may be a student in a university course who is studying parallel programming using the MPI (Message Passing Interface) API (Application Programming Interface). As with other Shibboleth applications, users contact the WebMPI interface, and then are redirected through the Shibboleth protocol to authenticate through the authentication mechanism of their home institutions. User attributes are passed to the WebMPI interface, which then determines if the user is authorized to use the cluster or not.

The current implementation of WebMPI is a prototype. The interface consists of a collection of HTML pages and CGI scripts that perform the user's commands on the underlying cluster resource. The current system is convenient for student programs and other types of small demonstration programs. However, it is limited for large production scientific applications.

⁸ Additional information on this application can be found in the Great Plains Network: Integrating Shibboleth, Grid and Bioinformatics at:
<http://archie.csce.uark.edu/gpn/publications.html>

One of the issues encountered in the development of WebMPI that does not come up in the same way for resources such as the GPN Repository is how to handle processing on the underlying cluster. In a normal MPI application, a user logs in to the head node of the Linux cluster using a local account and password. Any new files are created in the user's home directory and all processes that are created run under the user's account. The underlying Linux operating system protects the computer system from a stray process that could create too many files, or that creates files that are too large, or that could consume too much CPU time.

In contrast, one of the features of Shibboleth is that it allows the protection of user privacy. While it is possible to pass a user name or account within the Shibboleth architecture when it is desired to do so for a particular application, Shibboleth in general works by not revealing the user's name or account. Access is typically based on group membership, or the possession of a particular attribute. There are two ways this presents a challenge when integrating Shibboleth with MPI. First, there needs to be a way to map an incoming user to a subdirectory on the underlying cluster, and secondly, there needs to be a way to map an incoming user to an account in which processes may execute.

One of the attributes that can be maintained by the Identity Management system at the home institution is the PersonID (part of the



eduPerson schema). The PersonID is an opaque identifier that is guaranteed to be unique for a person. WebMPI maintains subdirectory integrity by mapping the PersonID to a subdirectory on the underlying cluster. By using a mapping in this way, a user may authenticate a second time and be mapped to the same user space representing the same subdirectory. For example, a user is able to start a long-running MPI application, and then return at a later time to view results. Note that for a user to be authorized to use WebMPI, the IdP at the home institution of the user must release the PersonID attribute to the WebMPI resource.

User-level MPI processes are handled in WebMPI by executing all MPI applications in a single account named the “webmpi” account. In the interface, a user requests the execution of an MPI program. Since WebMPI is a web application, the suEXEC feature of the Apache web server can be used to execute the MPI program in the webmpi account on behalf of the user. Results are maintained in the appropriate subdirectory. This technique is secure in that only users who authenticate through the Shibboleth interface are allowed to execute programs; however, it does not allow the logging of usage of individual users. Other solutions to the process-mapping problem are being explored.

Attributes

As the resources in the GPN federation have become more complex, the need has arisen for a structured way of managing the attributes that are required for access to these

resources. The EDUCAUSE/Internet2 eduPerson Task Force⁹ has defined a data structure (object class) that defines attributes that are useful for individuals in higher-education. Among the attributes are an individual’s institutional affiliation, and their relationship to the institution, such as faculty, student or staff. At a very high level, this provides a coarse-grained means for distinguishing groups within an institution, such as all faculty members or all students enrolled in a particular class during a particular semester. At this level, decisions about authorizations to utilize various services at an institution can be readily made.

The eduPerson Task Force identified the syntax and semantics of these attributes. The development of this object class is now managed by the MACE-Directory Working Group, which is encouraging widespread adoption of the attributes among institutions of higher-education. These attributes are common across institutions and as a proposed standard the defined object class is or can be quite useful to enable a wide variety of applications and services both within an institution and external to it.

The GPN/ETR group, upon reviewing the attribute fields, had a need for more fine-grained controls over authorizing access to specific, shared, collaborative resources and to services that span several institutions among the Great Plains states. The values for attributes for most fields in the eduPerson

⁹http://www.educause.edu/content.asp?PAGE_ID=949&bhcp=1H



object class are single-valued and/or predefined (e.g., faculty, staff, student, or member).

The eduPersonEntitlement Field

To accomplish the goals of the GPN/ETR project, an attribute that can take on various values and, in fact, be multi-valued is desired. The field that has the required properties is the eduPersonEntitlement field. Thus, the GPN/ETR group is focusing on the entitlement field to define the necessary values that facilitate the need for fine-grained decision-making when authorizing access to inter-institutional, collaborative resources. Use of the entitlement attribute in combination with other eduPerson attributes, Shibboleth, Apache authorization, and a portal application GPN has set the stage for fine-grained control of authorizing access to specific resources and services.

The entitlements are defined as LDAP attributes using the eduPersonEntitlement definition. The entitlement attribute permits multiple values. The entitlement attribute is a semicolon-separated string containing MACE registered values that are asserted and verified during the authorization process to grant or deny access to an entitlement dependent resource. It is possible to release attributes to some, but not all institutions. The SP must define what attributes it will accept, and from whom. An attribute acceptance policy might allow all GPN institutions to assert eduPersonEntitlement, but no others.ⁱⁱ The GPN access to resources can be further

mediated by a portal application that determines final access using the combination of entitlements that are asserted.ⁱⁱⁱ

Registration of the MACE Greatplains.net Namespace

The GPN/ETR team is defining an architecture predicated on the eduPersonEntitlement attributes defined in the GPN registered MACE NameSpace to support a regional collaboration environment among its members. The Great Plains Network (GPN) has registered the name *urn:mace:greatplains.net* with MACE. This name is the top level of a hierarchical namespace controlled by the GPN for use in its collaboration efforts. In the case of GPN, this namespace includes specific entitlement values that are used to provide fine-grained access control to GPN defined resources. There are currently four resources at two different institutions that require the use of eduPersonEntitlements.

Individuals who have authenticated through Shibboleth (at their home institution) and who have eduPersonEntitlements that match the greatplains.net defined entitlements are granted access to the defined resources or services. Individuals without such entitlements are denied access, even though they have been authenticated via Shibboleth from one of the collaborating institutions. Additional information on the GPN/ETR attribute architecture is provided in Appendix D.

As part of the MACE namespace registration process, an URL is provided to access online



documentation for the registered namespace.

In the case of the *greatplains.net* MACE namespace, the registered URL is:

<http://www.greatplains.net/mace-gpn>.^{iv}

The MACE registered namespace for *greatplains.net* is critically important to this project since it provides a persistent URN naming convention under control of the GPN/ETR collaborating institutions. This mechanism creates a virtual organization (VO) consisting of a wide variety of individuals from a collection of institutions that does not fall into the normal classifications for individuals in a typical identity management system within or across multiple institutions. For example, the VO can permit selected students, faculty and staff at various institutions to participate in the VO without granting access to all such groups of individuals from all of the institutions. In short, the defined entitlements provide a way to utilize middleware standards, while providing an extensible means for accommodating specific and unique needs of groups of individuals that can be easily tailored for fine-grained discriminating decisions implemented in application programs and systems.

Building Virtual Organizations

Synergistic Activities

Biomedical Sciences

A group of GPN researchers from member institutions has begun planning to enable biomedical application development and

collaboration using the developing GPN middleware infrastructure. This effort is in its infancy, but is due in part to the expanding efforts of the GPN to encourage researchers to become active in projects that enable applications of specific interest to the researchers.

Using the middleware infrastructure, the researchers can concentrate on the development and deployment of applications of biomedical software for research use. The middleware infrastructure also enables the group to utilize inter-institutional resources, such as grid technology, to further the individual research efforts. In fact, the GPN MACE entitlements BioSci and BioGrid were set up to support the efforts of this group and other groups in the future.

The biomedical sciences group is planning a pilot implementation to be used to prepare for submissions of research proposals to external funding agencies. This planning process includes selecting appropriate applications suited for this activity, developing a prototype pilot implementation and collecting data to be used in proposal writing.

Environmental Sciences

A second group of researchers in the area of environmental sciences, water resource modeling and watershed research is also keenly interested in using the developing middleware infrastructure in support of research. The environmental science group has a history of collaboration that precedes the GPN/ETR project. The broad-based water



modeling applications developed in the GPN environmental science research community. Some of the applications use data that is collected across a broad geographic region and shared among the researchers in the area. The needs of this virtual organization to share data, applications, and research results in an authorized manner are helping to drive the development of GPN middleware.

Managing Entitlements in VO Organizations

Defining entitlements and utilizing them in applications to provide fine-grained discrimination for authorization is only part of the problem of VO entitlement management. The management of the entitlements in identity management providers (IdP) across a virtual organization is particularly challenging. A large number of policy and technical decisions must be developed to allow entitlement data to be incorporated into separate IdPs governed by different business and policy models.

The GPN/ETR is cooperating with NMI-EDIT and Internet2/MACE Signet groups to look at the issues and means for VOs to authorize, request and manage the authorization data that must be incorporated into separate IdPs to be effective. For example, the GPN/ETR entitlement values must be contained in an IdP's identity management database for individuals authenticated at their home institution and who are members of the VO organization. The VO organization should be the one to authorize entitlements in a given IdP, but IdPs are reluctant to empower anyone

but their local identity management team to update anything in their database. Similarly, a single individual may have several identities and roles in an organization and it must be determined which identity is to be granted access in an external VO.

These issues are of significant interest to a wide range of institutions, government agencies, and funded research projects. The multiple institutions operating as a virtual organization in the GPN/ETR are in an excellent position to collaborate on these issues and investigate the evolving mechanisms in the GPN's live testbed.

Integration with Grid Computing Middleware

Grid computing has been one of the driving forces for the GPN/ETR group. Once the ability to use Shibboleth for authentication across institutions was accomplished, the ability to access shared resources and applications became an important part of the group's efforts. The utilization of Shibboleth authentication, MACE entitlement authorization capabilities and accessing grid computing resources that can be shared among the members of the GPN/ETR VO is key. In fact, the recent GPN annual meeting was devoted to all of these topics with presenters from around the country.

As much as possible, the GPN/ETR is incorporating standards-based products into their middleware infrastructure that will support collaborative efforts across the Great Plains and beyond. Efforts such as Condor, Globus,



GridShib, Signet and Grouper¹⁰ all have a role in the GPN efforts. A number of projects are evolving among the GPN institutions that incorporate these different high throughput and grid technologies.

Lessons Learned

The development and deployment of a middleware infrastructure in the GPN is an on-going project. The history of GPN has been to focus on cost reduction in the purchase or lease of infrastructure. In contrast, the GPN ETR project is an infrastructure-related project with a different set of priorities, including human capacity building, training and consulting, and the use of shared resources across campuses and state networks. As such, the challenges and limitations of the project have been largely in the area of human resources. A summary of the lessons the GPN/ETR team has learned in this area includes the following:

1) The tools are new and sometimes difficult to install and use. Collaboration and community support is required. And, if individuals are working collaboratively, the needed expertise can be effectively distributed among the collaborating institutions. Individuals are much more comfortable contacting colleagues they already know for help in installing and configuring a new tool. A high level of collaboration allows the project to move along much more quickly.

Collaboration and compatibility with the larger middleware and grid community is a necessity. The individual GPN institutions may want to consider joining InCommon to support trusted sharing of protected resources, and GPN will want to integrate its infrastructure in an appropriate way with that of InCommon. Similarly, the grid research projects at GPN institutions may also want to consider joining the Open Science Grid¹¹ or other grids that are based on similar technologies.

2) The middleware project will be limited by the level of support provided by the institutions in the region. For the project to really progress, the participating institutions must provide resources. Specifically, employees must be given time and encouragement to work on the project. In the case of staff employees, time must be allocated during the week that can be specifically devoted to the middleware project. In the case of faculty, the tenure reward system must recognize their contribution to the middleware project as evidence of productive research and teaching. The benefits of a middleware infrastructure are long-term, and so an institution must similarly take a long-term view of its contribution to the project and not expect an individual's efforts to immediately benefit the institution.

3) It is essential to remain aware of current events and changes within the broader middleware community. Even during the life of the ETR project, the capabilities and focus of the Shibboleth project changed to become

¹⁰NSF Middleware Initiative: [Hhttp://www.nsf-middleware.org/H](http://www.nsf-middleware.org/H)

¹¹ Open Science Grid: [Hhttp://opensciencegrid.org/H](http://opensciencegrid.org/H)



more grid-oriented. For example, the release of the GridShib software component for unifying Shibboleth and Globus security models is likely to impact the middleware structure of the GPN in the future.

Communication and constant education are needed.

Future Plans

The GPN ETR project has accomplished the original goal of the deployment of a middleware test bed on a small number of campuses. These deployments are largely in prototype and test status. However, a collaborative infrastructure has been developed that enables future middleware planning and deployment.

The next goal for the GPN regional middleware infrastructure is to move towards a production quality set of tools in support of research and education in the region.

Although this goal is simply stated, there are several steps that must be defined, planned, and accomplished. The most visible step that is likely to come next is the development of a GPN portal for access to regional resources in an authenticated and authorized manner using the Shibboleth infrastructure. This component and others will continue to be defined as the project team expands the middleware infrastructure in the Great Plains region.

There will likely be many new challenges. For instance:

- As the GPN moves toward a more production quality set of tools, policies will

need to be developed both within the virtual organization and at individual campuses for sharing resources.

- There will be a need for the implementation of technology solutions to support these policies.
- The management of privileges will become an important problem to solve. Member institutions at GPN are working with the Signet software and working group to better understand how user privileges in a diverse virtual organization can be managed across a range of applications.
- Timing the move to production. In the distributed environment it is possible that some components may move to “production-quality” more quickly than others. As GPN moves forward with prototype tools in the testbed, they plan to encourage as many new users as possible to use the available tools, while not discouraging them with components that may still be in a development phase.

Since the deployment of production-quality middleware tools will also require production-quality software, hardware, and maintenance, continued funding is also a challenge.

Institutions will want to see how the additional costs associated with these new production components may be offset by additional funds to the institution, either in the form of cost-savings because now some resources can be accessed remotely, or in the form of additional research that can be performed, or additional grants that can be acquired because of the



additional capability that is available to researchers at the institutions. New funding from such sources will be a necessity to move the project forward. Finally, GPN will need to consider how its middleware infrastructure will allow institutions to manage potentially different types of middleware technologies.

GPN is continuing strategic planning on a regional basis. Although the GPN ETR funded project has ended, regular meetings are continuing with interested middleware planners. The GPN ETR project has helped to provide a foundation upon which the GPN hopes to build a robust regional middleware infrastructure.

More Information

For more information about this GPN ETR Case Study is available at the GPN ETR web site¹² and also by contacting Amy Apon at aapon@uark.edu.



¹² <http://archie.csce.uark.edu/gpn/H>

^I The Shibboleth software package is layered on top of standard software environments. The IdP is a Java web application that runs in the Tomcat servlet container over the Apache web server. The Service Provider is somewhat more complex, but uses standard C/C++ and XML based software components.

^{II} Shibboleth by default disallows any institution from asserting attributes scoped to another institution. Also, an IdP may choose to only release certain values of an attribute to a particular SP. For example, a GPN SP might only be able to see GPN-related eduPersonEntitlement values, and not those related to other organizations.

In the Apache configuration for the SP, the required attributes are defined, and if the "ShibRequireAll" directive is specified, all attributes must be present. Otherwise, the default Apache behavior is to authorize access if any *one* of the attributes matches. These can be matched exactly, or a regular expression may be used to match a range of acceptable values. (Note: if regular expressions are used, extreme caution should be paid to ensuring unwanted matches do not mistakenly get accepted).

^{III} Apache will permit users asserting any GPN MACE registered entitlement. This is achieved using a regular expression. Once the user is at the portal, they may be granted access to one or more resources (or none, as appropriate) depending on what entitlements are asserted.

^{IV} This web site defines the namespace and the entitlement attributes defined for use by the GPN/ETR group. The documentation for MACE as well as the corresponding IETF RFC (3613) that MACE is based on is provided as links from the same web page.



Appendix A: Participating Regional Organizations and State Organizations

A. Regional Organizations

The Great Plains Network (GPN) is a consortium of member universities in seven states, dedicated to supporting scientific research and education through the use of networking technology. The GPN Consortium constructed a high-speed network to support the earth system science community among the member universities. That network interconnected member universities and then connected them to the greater Internet2 community via the Abilene network and, via Abilene, to high-speed networks on other continents. Since 1997, both network configuration and network speed have evolved. The role of GPN has also evolved. GPN now provides a host of technical and non-technical, research and education related services to the university community. The GPN Consortium has a Technical Team, composed of experts from member universities, who advise on network implementation and operation. GPN also has an Earth Sciences Advisory Team whose members evaluate the infrastructure, plan collaborative research, and make recommendations for infrastructure improvements. Greg Monaco (co-PI and GPN Director for Research), and several GPN

Executive Council members have been active collaborators on this project.

MIDnet is a regional network to connect researchers in Arkansas, Iowa, Kansas, Missouri, Nebraska, Oklahoma and South Dakota. In the spring of 1986, a consortium of midwestern universities requested funding from the National Science Foundation to create a regional computer network for the purpose of accessing the NSF-funded supercomputer centers and exchanging information with other researchers. In the summer of 1986, the NSF funded the proposal for the creation of MIDNet. In September of 1987 MIDnet became the first of the regional networks to become fully operational. MIDnet's original focus was to create a network for accessing and exchanging information and throughout its history, information exchange continued to be a major focus. Semi-annual member conferences were important vehicles for fostering information exchange and they are considered to be the legacy of MIDnet. After MIDnet assets were acquired by Global Internet, a Palo Alto, California start-up, the original board of directors of MIDnet was reorganized as the MIDnet Research and Higher Education Advisory Council. MIDnet, Inc. continues to serve the research and education community as a quality provider of



network education and information exchange. Carol Farnham, the Executive Director of MIDnet, as well as several members of the MIDnet Board of Directors have been active collaborators in developing this project.

B. State Organizations

ARKnet is the academic/research computer network of Arkansas. In May 1991, the University of Arkansas, Fayetteville, received an award under the National Science Foundation's "Connections to NSFnet" program that allowed it to create ARKnet. The nineteen state colleges and universities were provided Internet access through the grant. Two additional institutions joined later to become the charter members of the new ARKnet confederation. ARKnet is organized as a not-for-profit confederation managed by its Board of Directors and governed by a set of bylaws. Each Director fills a position according to institutional categories as specified in the ARKnet bylaws. Directors are elected from the Institutional Representatives appointed by each member institution.

KanREN is a non-profit consortium of colleges, universities, school districts and other organizations in Kansas, organized for the purpose of facilitating communication among them, and providing themselves with connectivity to the Internet via a statewide TCP/IP network. KanREN is an independent, not-for-profit Kansas corporation. Membership in KanREN is open to any college, university, library, or school district in

the state of Kansas. Other non-profit organizations may join the consortium subject to the approval of the KanREN executive committee. KanREN is an Internet2 Sponsored Education Group Participant (SEGP) and a Kan-Ed peering partner. KanREN is affiliated with the Great Plains Network and a member of Net@EDU, the policy making division of EDUCAUSE.

Kan-ed has three objectives: to build a private, secure network to which members (Kansas hospitals, K-12 schools, libraries, and higher education institutions) can connect for access to high-speed content and services and a stable platform for video conferencing; to provide members with subsidies to help reduce their fees for Internet 1 (commercial Internet) access from local providers; to provide quality content and services that enhance the private network that Kan-ed members can use through their commercial or private Internet connection.

MOREnet, the Missouri Research and Education Network, provides Internet connectivity, access to Internet2, technical support, videoconferencing services and training to Missouri's K-12 schools, colleges and universities, public libraries, health care, state government and other affiliated organizations. Established in 1991, MOREnet operates as a separate unit within the University of Missouri System, and is based in Columbia, Mo. The MOREnet network is the foundation infrastructure. Members of the education community interact with each other



via data and video services; public sector business applications are built and conducted on it; and Missouri citizens interact with their state government through it. MOREnet is not a private Internet service provider and does not provide services, including dial-up access, on an individual basis.

OneNet began in 1992 when voters in Oklahoma approved a statewide capital bond issue that provided \$14 million for the implementation of a statewide telecommunications network. In late 1995, the State Regents approved the OneNet business plan and began implementation in 1996. OneNet initially focused on establishing the necessary [hub sites](#) throughout Oklahoma to provide the infrastructure necessary to support the high-speed telecommunications network. In addition, it moved aggressively to establish an equitable rate structure and

enroll customers. State-of-the-art technology and a highly dedicated staff currently provide high-speed communications to a variety of Oklahoma entities such as: public and vocational-technical schools; colleges and universities; public libraries; local, tribal, state and federal governments; court systems; rural health care delivery systems; and programs engaged in research.

The South Dakota Board of Regents has constitutional authority to govern the system of public higher education in the State of South Dakota. Supported by an Executive Director and staff, including a technical staff, the Board provides leadership and sets policies for the programs and services delivered through its six universities and two special schools.



Appendix B: Participating Campuses

University of Arkansas (UAF):

UAF utilizes SunOne (iPlanet) Directory Server to provide a central LDAP directory for the campus. This directory receives automated updates through metadirectory software developed locally to populate and update entries from their business and student information systems. UAF utilizes the directory for authentication of key open systems in its central computing facility. UAF has coordinated with other colleges and departments within the university to do the same with a number of their servers. The same metadirectory also feeds a Microsoft Active Directory for the Windows environment.

University of Kansas (KU):

The University of Kansas (KU) makes extensive use of campus middleware systems for identification, authentication, and authorization services. KU employs LDAP-based authentication using a KuPerson schema developed as an extension of the eduPerson schema. Behind this KU has a comprehensive Oracle-based repository generated and maintained from several primary campus data sources. In the future KU intends to continue development based on NMI-EDIT activities, including the use of Shibboleth, and plans to continue participating in the NMI-EDIT CAMP sessions. KU is actively investigating PKI deployment, and has an initial system for distribution of end-

user certificates (locally signed) to KU employees and students.

University of Missouri-Columbia (MU):

The University of Missouri-Columbia utilizes a unified campus-wide authentication scheme based on Microsoft's Active Directory and MIT's Kerberos. Active Directory is used throughout the University to provide access to Microsoft Exchange and other administrative and academic services. In the future MU intends to bridge the campus and University authentication services to the evolving systems being developed on a national scale, such as NMI-EDIT and Shibboleth as well as the Grid computing environment. The MU intent is to provide a "seamless" transition between local and global authentication and authorization as well as resource sharing activities. It is vitally important that MU is able to actively participate nationally and globally and the use of middleware is critical in achieving this end.

University of Nebraska – Lincoln:

UNL is home to the PrairieFire supercomputer and other grid computing facilities. UNL is also embarking on campus-wide wireless network connectivity. In addition, UNL has deployed three Access Grid multimedia videoconferencing facilities in recent years. Currently the campus is embarking on middleware activities such as cross campus authentication/authorization.



University of Oklahoma (OU):

Currently OU has engaged in the following middleware-related activities: (1) reduced the master account management database to a single Oracle database; (2) implemented standard LDAP and Microsoft Active Directory Services for user authentication and authorization. In addition, (3) OU is currently researching the deployment of a PKI and Shibboleth to augment current authentication and authorization infrastructure. The OU Supercomputing Center for Education & Research (OSCER), in cooperation with the Oklahoma High Energy Physics community, has led the OU campus in research middleware, having installed Globus, Condor-G, the Virtual Data Toolkit and related technologies. Under a National Science Foundation Major Research Instrumentation grant, OSCER is about to deploy an Itanium2 cluster whose primary role will be as a development platform for Grid-enabled science and engineering applications.

North Dakota State University (NDSU):

North Dakota State University has been actively pursuing IAA solutions since the mid-1990's when NDSU migrated to a distributed computing architecture. Part of their migration included development of an IAA solution called *Hurderos*. *Hurderos* is a true IAA system supporting identity management, authentication and differential authorization. An API (*KerDAP*) was developed and used to modify many of NDSU's server-based applications including email (IMAP), web proxy, RADIUS, etc. NDSU employs *Hurderos* to provide centralized services to six of the

eleven North Dakota University System colleges and universities and all of the North Dakota K-12 community (over 70,000 users). Future plans for *Hurderos* include integration with the state's new PeopleSoft ERP system and incorporating the NMI-EDIT recommendations including support for Shibboleth.

Peter Kiewit Institute (PKI):

The Peter Kiewit Institute (Omaha, Nebraska) is home to the University of Nebraska-Lincoln's College of Engineering and Technology and the University of Nebraska at Omaha's College of Information Science and Technology. The Peter Kiewit Institute is designed to help meet the needs of the nation's technology and engineering firms by providing a top-flight education to students interested in pursuing careers in information science, technology and engineering.

University of South Dakota (USD):

Currently The University of South Dakota is involved with the following activities with respect to middleware: USD has participated with the implementation of Active Directory with the rest of the South Dakota Regental campuses towards the goal of implementing inter-campus single sign on within South Dakota public universities. Active Directory doesn't integrate all of their 'islands' of authentication and authorization. Nor does it provide a regional solution for sharing resources. In addition USD has been active in implementing an enterprise directory service based on Sun Microsystems directory server for the last 18-24 months. USD



libraries rely heavily on content provided by on-line database providers and USD sees Shibboleth as a key technology to being able to continue provide access to these resources to their students, faculty and staff.

South Dakota State University:

Middleware implementation at SDSU is in the early stages of development. While LDAP, and other identification and authentication directories and databases, have been available for several years at SDSU, the broad use of these resources for controlling access to computer resources has been limited. An Active Directory (AD) implementation, coordinated through Regents Information System with the other five South Dakota public universities, is nearly complete at SDSU. They will be investigating ways that this AD information resource might be further leveraged for identification, authentication and authorization (IAA). An Intranet at SDSU is being expanded to provide access to MIS and

other university critical information and resources. Over the next one to two years, it is our goal to investigate and then integrate IAA into all aspects of this Intranet. SDSU has a supercomputer level cluster that will be shared with other research universities in the state. Middleware implementation for access to this and other supercomputing and grid computing in the region will be pursued.

Additional campuses to be included:

Wichita State University, Emporia State University, Creighton University, Iowa State University, Kansas State University, Oklahoma State University, University of Iowa, University of North Dakota, South Dakota School of Mines and Technology, University of Tulsa, Little Priest Tribal College, University of Oklahoma Medical School, University of Missouri at Rolla, University of Missouri at St. Louis, University of Missouri at Kansas City, University of Arkansas at Little Rock, University of Arkansas Medical School.



Appendix C: Project Plan Timelines

TABLE 1: BUILDING THE REGIONAL MIDDLEWARE INFRASTRUCTURE TIMELINE

Phase I (Year 1)	QUARTER 1	QUARTER 2	QUARTER 3	QUARTER 4
Project Team Education	Project Staff, Campus Staff attend Camp Shibboleth			
Strategic Planning Committee	Formalize & Initiate Meetings	Engage additional schools in region	Draft Strategic Plan	Finalize Strategic Plan
Implementation	Shibboleth at University of Kansas		To be determined (Case Study II)	
Campus Assessment	1. Develop assessment tool 2. Initiate assessment	Circulate preliminary assessment results	Refine results	
Interoperability Testing		Install various middleware environments	Interoperability testing	Circulate preliminary results
Consulting		Build Model and Publicize Consulting Availability	Initiate Regional Consultation	
Regional Middleware Workshops		Best Practice I Campus Updates KU Case Study Strategic Planning Process		Best Practice II Case Study II Campus Updates Interoperability Results
Educational Outreach Activities		1. GPN/Midnet Middleware Technical Training Workshop 2. Oklahoma Supercomputing Symposium 3. Internet2 BoF	1. GPN/MIDnet Annual Meeting - Middleware Track 2. Middleware & Grid Computing Technical Training Workshop	Presentation at Internet2 Meeting Annual Report Case Studies Published



Appendix D: Building an Attribute Architecture

Shibboleth is used for authentication into the "virtual organization" (*greatplains.net*) environment. The *urn:mace:greatplains.net* NameSpace is used for required authorizations to access the collaboration resources defined within the NameSpace via Shibboleth and eduPerson released entitlements. It is important to note that the enforcement of the entitlement rules for access is enforced in a split responsibility fashion. The first part of the entitlement syntax (*urn:mace:greatplains.net*) is enforced by the Shibboleth target Apache web server. That is, if the prefix of the entitlement for the GPN MACE NameSpace does not appear in the entitlement list at authentication time, access to the Shibboleth target is denied. The last part of the NameSpace entitlement (everything following the final colon in each entitlement in the list of entitlements asserted during the authentication) is used to enforce the specific authorizations an entity has within the defined entitlement NameSpace. See below for the currently defined entitlements.

The presently defined entitlements consist of two groups; the entitlements requested for use by the University of Missouri - Columbia and the entitlements requested for use by the University of Arkansas. Conceptually, these entitlements are hierarchical and interoperable. And, globally these entitlements permit fine-grained control over selected resources or capabilities offered to

users located at several institutions located in the Great Plains region.

The architecture and definitions presently active are accessible at:

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

The entitlements defined include:

❖ **urn:mace:greatplains.net:biosci**

The BioSci attribute allows authenticated identities to access and utilize resources to support research activities in the biological and life sciences among the member institutions.

❖ **urn:mace:greatplains.net:biogrid**

The BioGrid attribute allows authenticated identities to access and utilize region-wide grid computing resources to support research activities requiring grid computing access.

❖ **urn:mace:greatplains.net:repository**

The Repository attribute allows authenticated identities to access and utilize a region-wide data repository for sharing documents, files and data among the participating members.

❖ **urn:mace:greatplains.net:uark.edu:webmpi**

The WebMPI attribute allows authenticated identities to access and utilize the grid computing cluster at the University of Arkansas to develop, test, and run MPI-based parallel programs.



The three entitlements: **BioSci**, **BioGrid**, and **Repository** have a hierarchical relationship. **BioSci** is the superior (top level) entitlement that incorporates the **BioGrid** and **Repository** entitlements. That is, any authenticated entity that incorporates the BioSci entitlement automatically is presumed to also have the BioGrid and Repository entitlements as well. However, an authenticated entity with the BioGrid entitlement does not incorporate the BioSci entitlement or the Repository entitlement. The same is true for the Repository entitlement. Namely, having the Repository attribute does not incorporate either the BioSci or the BioGrid attribute for authorization purposes.

The **WebMPI** entitlement has an interoperable relationship with the BioSci entitlement. Namely, at the University of Arkansas, an authenticated entity with the WebMPI attribute is granted access to the grid computing resource for developing MPI programs on a cluster machine. However, another authenticated entity with the BioSci attribute will be authorized for the

WebMPI attribute when required or needed. (**Note:** this interoperation capability is not fully functional at this time.)

Details of the meaning of the specific entitlements that have been defined can be found by accessing the appropriate links in the attribute table found at:

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

These definitions are in active development and are subject to change at any time. The URN attributes are persistent, but the details of the authorizations they carry may change.

At this time, the BioSci, BioGrid, and Repository MACE entitlement attributes are associated with the Shibboleth Target:

<https://crick.rnet.missouri.edu/GPN>. The

WebMPI MACE entitlement is associated with the Shibboleth Target:

<http://webmpi.csce.uark.edu>.

