

NMI Component Testing Guidelines

Pertaining to: NMI Release 3 (Release date: April 28, 2003)

May 2, 2003

This packet contains NMI Component Testing Guidelines for individual components released as part of NMI Release 3.0. The information was prepared by the NMI Integration Testbed Manager working in cooperation with the NMI Testbed-Council to represent the interests of the NMI Management team and also relevant component developers. This information is intended to provide NMI Integration Testbed sites with sufficient guidance per component to enable evaluation of any given component at their site as used with actual projects and applications. It also specifies reporting mechanisms designed to enable the capture, aggregation, and analysis of participant sites' evaluations.

NMI Testbed site representatives may undertake evaluation of components themselves or may delegate to or collaborate with others at their sites having useful expertise and experience to evaluate specific components. Instructions are provided for noting the name and position of the additional evaluator(s) for cases where feedback is originating from someone other than the NMI Testbed site representative.

Though specific actions are listed for the evaluation of individual components, those participating in evaluation should also consider and operate within the context of the general categories of evaluation for NMI components, as applicable. These general categories of evaluation are:

- Integration at and distribution to workstations and other endpoint resources
- Interaction with commonly deployed campus infrastructure
- Vertical discipline integration within communities of users
- Component scalability and consistency
- To the greatest extent possible, all evaluations should involve real users in realistic application scenarios and the integrated use of several middleware components

A new and updated version of these NMI Component Testing Guidelines will be made available through the NMI Testbed Manager to the NMI Integration Testbed sites prior each NMI Release to enable the start of the formal integration testing cycle.

For additional information on the components in NMI Release 3, see <http://www.nsf-middleware.org/NMIR3/components.asp>.

NMI Release 3 Components:

GRIDS Center components

New for R3

- 1. MyProxy v0.5.2**
- 2. MPICH-G2**

Updated for R3

- 3. NMI Client and Server Bundles**
- 4. Globus Toolkit v2.2.4**
- 5. Condor-G v6.4.8**
- 6. Network Weather Service v2.3**
- 7. KX.509 and KCA (for Globus) v1.0**
- 8. GSI-OpenSSH v1.8**
- 9. Grid Packaging Tools v3.0**
- 10. Gridconfig Tools v0.1.3**

NMI-EDIT components

New for R3

- 1. PERMIS - PriviEge and Role Management Infrastructure Standards Validation – v1.2**
- 2. Look - The LDAP operational ORCA "k"ollector – v0.9**
- 3. SAGE - Service for Authorized Group Editing – draft**
- 4. Enterprise Directory Implementation Roadmap – draft**

Updated for R3

- 5. LDAP Analyzer – v1.0**
- 6. Shibboleth – v1.0**
- 7. OpenSAML – v0.9**

Unchanged for R3

- 8. KX.509 and KCA v1.0 (standalone) v1.0**
- 9. Certificate Profile Maker v1.1**
- 10. Pubcookie v3.0**
- 11. eduPerson (200210)**
- 12. eduOrg (200210)**
- 13. commObject, October 2002**
- 14. Certificate Profile Registry**
- 15. Practices in Directory Groups, October 2002**
- 16. LDAP Recipe, October 2002**
- 17. Metadirectory Practices for Enterprise Directories in Higher Education, October 2002**
- 18. Shibboleth Architecture v.5, May 2002**
- 19. Higher Education PKI (HEPKI) Model Campus Certificate Policy**
- 20. Lightweight Campus Certificate Policy and Practice, April 2002**

Component:	MyProxy v0.5.2
<i>New for R3</i>	MyProxy is a credential repository for the Grid. Storing your Grid credentials in a MyProxy repository allows you to retrieve a proxy credential whenever and wherever you need one, without worrying about managing private key and certificate files. Using a standard web browser, you can connect to a Grid portal and allow the portal to retrieve a proxy credential for you to access Grid resources on your behalf. You can also allow trusted servers to renew your proxy credential using MyProxy, so, for example, your long-running tasks don't fail because of an expired proxy credential.
Pre-requisites:	A GRIDS Center Software Suite supported operating system.
Deadline:	July 1, 2003
Evaluation & Reporting:	<ul style="list-style-type: none"> • Verify MyProxy installation procedures and documentation. Note the system specifications for each installation performed. • Deploy a Grid portal for a targeted application or community using MyProxy. Consider using the Grid Portal Development Kit or the Grid Portal Toolkit. Report on your experience. • Evaluate using MyProxy for general-purpose GSI credential management, as an alternative to user-managed long-term credentials. Encourage users to store their credentials in the MyProxy repository and retrieve proxy credentials from MyProxy. Compare usability and support costs for user-managed long-term credentials, MyProxy-managed credentials, and (if possible) KX.509/KCA credentials. Consider performing a security audit of your current GSI credential management solution. Are users choosing good GSI passphrases? Are long-lived GSI credentials stored unencrypted on insecure systems? • Discuss the feasibility of credential repositories with local security personnel and partner sites. Will sites allow (or even prefer?) user credentials to be stored in a credential repository, in contrast to user-managed credentials? Can a credential repository alleviate security concerns with user-managed credentials? This can be combined with a discussion about KX.509/KCA (or online Certificate Authorities in general). • Consider integrating a credential repository with your Certificate Authority (if you have one), where users' credentials are loaded into the repository on their behalf, potentially simplifying PKI enrollment. • If you have an existing credential repository, compare it with MyProxy. • Describe your experiences with the Grid Security Infrastructure. What are the primary usability issues and support costs? What additional tools are needed? <p>As bugs or enhancement suggestions are identified throughout the evaluation period, please report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed MyProxy [short problem description]</p> <p>Keep a summary list of all bug/enhancement reported for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-MyProxy.doc</p>
Support:	NMI developers' discussion list (nmi-developer@nsf-middleware.org). To subscribe, send email to majordomo@nsf-middleware.org with a message body of "subscribe nmi-developer" (without quotes).

Component:	MPICH-G2 v1.2.5.1
<i>New for R3</i>	MPICH-G2 is a grid-enabled implementation of the MPI v1.1 standard based on the popular MPICH library developed at Argonne National Laboratory. Using services from the Globus Toolkit(R) (e.g., job startup, security) MPICH-G2 allows you to couple multiple machines, potentially of different architectures, to run MPI applications. MPICH-G2 automatically converts data in messages sent between machines of different architectures and supports multi-protocol communication by automatically selecting TCP for inter-machine messaging and (where available) vendor-supplied MPI for intra-machine messaging.
Pre-requisites:	GPT as part of NMI-R3.
Deadline:	July 1, 2003
Evaluation & Reporting:	<p>The steps described in this section help to confirm that you have successfully installed MPICH-G2 by having you compile and execute a small MPI program.</p> <ul style="list-style-type: none"> • Follow the instructions to acquire and install MPICH-G2 from the NMI website. Be sure to follow the instructions and edit the bin/machines file by placing the name of the Globus gatekeeper you are running this verification test on. • Acquire a Globus certificate (i.e., your Globus security credential that identifies you) from a Globus Certificate Authority (see http://www.globus.org for details) and make sure that your Globus certificate is in the Globus gridmap file on the machine that you are testing on. • Acquire the program ring.c from the NMI MPICH-G2 page and follow the instructions there to make and run the program. The correct output from that test can also be found on the NMI MPICH-G2 page. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these as they are discovered to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-G2.doc</p>
Support:	NMI developers' discussion list (nmi-developer@nsf-middleware.org). To subscribe, send email to majordomo@nsf-middleware.org with a message body of "subscribe nmi-developer" (without quotes).

Component:	NMI Client and Server Bundles v3.0
<i>Updated for R3</i>	The NMI Client and Server Bundles are an aggregate of all of the software components in the Grids Center Software Suite. This integrated package can help make installation and configuration easier for those who want to implement all or most of the technologies in this set. (Please review the NMI Server documentation for additional information on how to implement this software.)
Pre-requisites:	Pre-requisites are as applicable to the individual components being installed.
Deadline:	July 1, 2003
Evaluation & Reporting:	<p>Use the client/server bundle to install and configure GRIDS Center software for projects at your site and provide the following details for each installation performed:</p> <ol style="list-style-type: none"> 1. Brief description of the project this installation will support, including the specific activities that grid computing will support. 2. List of specific components being installed and configured. 3. Approximate time required for installation and configuration. 4. Assessment of the ease and accuracy of installation and configuration. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, please report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reported for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-Bundle.doc</p>
Support:	NMI developers' discussion list (nmi-developer@nsf-middleware.org). To subscribe, send email to majordomo@nsf-middleware.org with a message body of "subscribe nmi-developer" (without quotes).

Component:	Globus Toolkit v2.2.4
<i>Updated for R3</i>	The de facto standard for Grid computing, the Globus Toolkit is an open-source collection of modular "bag of technologies" that simplifies collaboration across dynamic, multi-institutional virtual organizations. It includes tools for authentication, scheduling, file transfer and resource description.
Pre-requisites:	Operating System: Red Hat 7.2 or 7.3 on IA32, or Solaris 8 on Sparc, or Red Hat on IA64. More information is available at: http://www.nsf-middleware.org/documentation/GlobusToolkit/
Deadline:	July 1, 2003
Evaluation & Reporting:	<ul style="list-style-type: none"> • Verify installation procedures and documentation as part of the general NMI-R3 packaging installation and separately. Note the system specifications for each installation performed. • Identify campus enterprise components or services (e.g., directory services, user accounts, supercomputer schedulers, etc.) that would be useful to integrate with specific Globus Toolkit components (e.g., MDS, GSI, GRAM) for resource management, security, information services and data management, and describe the targeted benefits of integration. • Identify and briefly describe scientific projects or applications at your site that are not currently using the Globus Toolkit but could benefit from doing so, and describe the anticipated benefits of usage. If steps towards usage are planned within the next 6 months, include an estimated timeline for implementation. • Install and use this version of the Globus Toolkit within scientific projects or applications at your site. For each project or application, describe the frequency and type of usage (specific components used, actions enabled) and the benefits derived. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-Globus.doc</p>
Support:	NMI developers' discussion list (nmi-developer@nsf-middleware.org). To subscribe, send email to majordomo@nsf-middleware.org with a message body of "subscribe nmi-developer" (without quotes).

Component:	Condor-G v6.5.1
<i>Updated for R3</i>	Condor-G is a computation management agent for the Grid – a marriage of technologies from the Condor project and the Globus project.
Pre-requisites:	<p>Operating System: Red Hat 7.2 or 7.3 on IA32, or Solaris 8 on Sparc, or Red Hat on IA64.</p> <p>Grid credentials and authorization, either on a locally constructed Grid or an already-established Grid such as the PACI resources, NASA IPG, or DOE Science Grid.</p> <p>Willingness to occasionally replace software with patches from the NMI developers.</p> <p>More information at: http://www.nsf-middleware.org/documentation/NMI-R2/0/CondorG/</p>
Deadline:	July 1, 2003
Evaluation & Reporting:	<ul style="list-style-type: none"> • Verify installation procedures and documentation. Note the system specifications for each installation performed. • Identify and briefly describe scientific projects or applications at your site that are not currently using Condor-G but could benefit from doing so, and describe the anticipated benefits of usage. If steps towards usage are planned within the next 6 months, include an estimated timeline for implementation. • Exercise Condor-G with other NMI-R3 components such as the Globus Toolkit and Kx509, and within scientific projects or applications at your site. Routine network and remote resource failures should be considered normal and automatically recoverable. For each exercise or project activity, describe the frequency and type of usage (specific components used, actions enabled) and the benefits derived. • Exercise the use of higher level tools such as the Condor DAGMan for managing Grid jobs within scientific projects or applications at your site. Describe the frequency and type of usage (specific components used, actions enabled) and the benefits derived. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-Condor-G.doc</p>
Support:	NMI developers' discussion list (nmi-developer@nsf-middleware.org). To subscribe, send email to majordomo@nsf-middleware.org with a message body of "subscribe nmi-developer" (without quotes).

<p>Component:</p> <p><i>Updated for R3</i></p>	<p>Network Weather Service v2.3</p> <p>The Network Weather Service is a distributed system that periodically monitors and dynamically forecasts the performance various network and computational resources can deliver over a given time interval. The service operates a distributed set of performance sensors (network monitors, CPU monitors, etc.) from which it gathers readings of the instantaneous conditions. It then uses numerical models to generate forecasts of what the conditions will be for a given time frame.</p>
<p>Pre-requisites:</p>	<p>Operating System: Red Hat 7.2 or 7.3 on IA32, or Solaris 8 on Sparc, or Red Hat on IA64.</p> <p>To take advantage of the services that NWS provides, knowledge of the local network is useful but not necessary. Firewalls and Network Access Translation (NAT) services can adversely affect the reachability of parts of NWS.</p>
<p>Deadline:</p>	<p>July 1, 2003</p>
<p>Evaluation & Reporting:</p>	<ul style="list-style-type: none"> • Verify installation procedures and documentation. Note the system specifications for each installation performed. • Provide feedback on configuration and management of NWS. • Identify and briefly describe scientific projects or applications at your site that are not currently using NWS but could benefit from doing so, and describe the anticipated benefits of usage. If steps towards usage are planned within the next 6 months, include an estimated timeline for implementation. • Exercise and describe interoperability of NWS with other NMI-R3 components and within scientific projects or applications at your site. Whenever feasible, this should be achieved with specific applications such as those developed for large-scale Grid deployments such as iVDGL, PPDG, GriPhyN, NEES, etc. For each exercise, describe the frequency and type of usage (specific components used, actions enabled) and the benefits derived. • Define how the NWS components in the following areas interact with the campus enterprise (e.g., directory services): Resource Management, Security, Information Services, Data Management. Devote particular attention to security aspects, including use of NWS in firewall and NAT conditions. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-NWS.doc</p>
<p>Support:</p>	<p>NMI developers' discussion list (nmi-developer@nsf-middleware.org). To subscribe, send email to majordomo@nsf-middleware.org with a message body of "subscribe nmi-developer" (without quotes).</p>

<p>Component:</p> <p><i>Updated for R3</i></p>	<p>KX.509 and KCA (for Globus) v1.0</p> <p>KX.509 and KCA provide a bridge between a Kerberos and PKI infrastructure. This technology is included in NMI-R3 to enable the PKI-based security infrastructure of the Globus Toolkit to integrate with Kerberos-based authentication implemented at university campuses. KCA 1.0 (Kerberosized Certificate Authority) receives a Kerberos ticket and issues a short-term PKI certificate. KX.509 1.0 is the desktop client that issues a request to the KCA and manages the returned certificate.</p>
<p>Pre-requisites:</p>	<p>Globus Toolkit 2.2.4, as part of NMI-R3.</p> <p>Kerberos infrastructure in place on campus, without PKI Certificate Authority (CA).</p> <p>Operating System: Red Hat 7.2 or 7.3 on IA32, or Solaris 8 on Sparc, or Red Hat on IA64.</p> <p>More information at: http://www.nsf-middleware.org/documentation/KX509KCA/index.html</p>
<p>Deadline:</p>	<p>July 1, 2003</p>
<p>Evaluation & Reporting:</p>	<ul style="list-style-type: none"> • Verify installation procedures and documentation. Note the system specifications for each installation performed. • Identify and briefly describe scientific projects or applications at your site that use grid applications but are not currently authenticated through the campus enterprise infrastructure but could benefit from doing so. If steps towards usage are planned within the next 6 months, include an estimated timeline for implementation. • Due to the growing need for Grids to work with Kerberos-based sites, a significant goal of the NMI testbed is to work through issues of campuses authenticating with Kerberos credentials that can then be used in GSI space. Demonstrate and describe the capability of researchers at your site participating in such projects (e.g., iVDGL, PPDG, GriPhyN) to do the following: 1) authenticate locally using Kerberos, 2) map through KX.509 to a GSI credential, 3) undertake all normal Grid project activities by presenting the credential to a DOE Science Grid CA. Demonstrate and describe this same capability with credentials as presented to relevant EU Datagrid CAs. • Explore/negotiate security policy with the campus Kerberos authority and the CA's of science projects involving researchers at your campus to determine if campus Kerberos credentials can be mapped into GSI credentials that will be accepted by CA's of existing and upcoming Grid projects. Describe the outcome of these discussions. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-KCA-KX509(G).doc</p>
<p>Support:</p>	<p>NMI developers' discussion list (nmi-developer@nsf-middleware.org). To subscribe, send email to majordomo@nsf-middleware.org with a message body of "subscribe</p>

| nmi-developer" (without quotes).

Component:	GSI-OpenSSH v2.0
<i>Updated for R3</i>	GSI-OpenSSH is a modified version of OpenSSH that adds support for GSI authentication, providing a single sign-on remote login capability for the Grid. It can be used to login to remote systems and transfer files between systems without entering a password, relying instead on a valid GSI credential for operations requiring authentication. It provides a single sign-on capability since it can also forward GSI credentials to the remote system on login, so GSI commands (including GSI-OpenSSH commands) can be used on a remote system without the need to manually create a new GSI proxy credential on that system.
Pre-requisites:	<p>Operating System: Red Hat 7.2 or 7.3 on IA32, or Solaris 8 on Sparc, or Red Hat on IA64.</p> <p>Grid credentials and authorization, either on a locally constructed grid or an already-established Grid.</p> <p>Willingness to occasionally replace software with updates from the NMI developers.</p>
Deadline:	July 1, 2003
Evaluation & Reporting:	<ul style="list-style-type: none"> • Verify installation procedures and documentation. Note the system specifications for each installation performed. • Exercise the tests provided in the verification section of the NMI GSI-OpenSSH documentation. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-GSI-OpenSSH.doc</p>
Support:	NMI developers' discussion list (nmi-developer@nsf-middleware.org). To subscribe, send email to majordomo@nsf-middleware.org with a message body of "subscribe nmi-developer" (without quotes).

Component:	Grid Packaging Tools v3.0
<i>Updated for R3</i>	The Grid Packaging Tools (GPT) are a collection of packaging tools built around an XML-based packaging data format. This format provides a straight forward way to define complex dependency and compatibility relationships between packages. The tools provide a means for developers to easily define the packaging data and include it as part of their source code distribution. Binary packages can be automatically generated from this data. The packages defined by GPT are compatible with other packages and can easily be converted. GPT provides tools that enable collections of packages to be built and/or installed. It also provides a package manager for those systems that do not have one.
Pre-requisites:	Operating System: Red Hat 7.2 or 7.3 on IA32, or Solaris 8 on Sparc, or Red Hat on IA64.
Deadline:	July 1, 2003
Evaluation & Reporting:	<ul style="list-style-type: none"> • First complete the installation and verification procedures. Any problems with the documentation should be reported. • Completing the installation of all other GRIDs components without problems is a sufficient test for GPT. To determine whether the installation is complete run the following command which should tell you what components are installed: • <code>\$GPT_LOCATION/sbin/gpt-query -what-bundles</code> • The following command should tell you whether the installation is complete or not. Any missing, mis-versioned, or unconfigured software will be reported: • <code>\$GPT_LOCATION/sbin/gpt-verify</code>
Support:	NMI developers' discussion list (nmi-developer@nsf-middleware.org). To subscribe, send email to majordomo@nsf-middleware.org with a message body of "subscribe nmi-developer" (without quotes).

Component:	Gridconfig Tools v0.1.3
<i>Updated for R3</i>	Gridconfig tools is a collection of configuration tools that manages the configuration for NMI software components. It provides an easy way to generate and regenerate configuration files in native formats, and to ensure configuration consistency.
Pre-requisites:	<p>Operating System:</p> <ul style="list-style-type: none"> Red Hat 7.2 or 7.3 on IA32 Red Hat 7.2 on IA64 SuSe 8.1 Solaris 8 on Sparc. <p>One machine on the site needs to run MySQL server software, Each machine where GridConfig is installed requires MySQL client software. See specific instructions in documentation.</p>
Deadline:	July 1, 2003
Evaluation & Reporting:	<ul style="list-style-type: none"> • Verify installation procedures and documentation. Note the system specifications for each installation performed. • Exercise the capability of users to generate valid configuration files that are needed by all NMI components. Summarize the frequency and outcome of these attempts. • Exercise the capability of users to re-generate valid configuration files after changing parameters for any subset of components. Summarize the frequency and outcome of these attempts. • Verify that created configuration files are equivalent to those produced by GPT for an equivalent setup and document any discrepancies and areas of improvement. Particular areas of interest include ease and speed of configuration/reconfiguration, user interface interaction, enumeration of configurations and issues which Gridconfig does not currently anticipate. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-GridConfig.doc</p>
Support:	NMI developers' discussion list (nmi-developer@nsf-middleware.org). To subscribe, send email to majordomo@nsf-middleware.org with a message body of "subscribe nmi-developer" (without quotes).

<p>Component:</p> <p><i>New for R3</i></p>	<p>PERMIS - PriviEge and Role Management Infrastructure Standards Validation</p> <p>The PERMIS authorization decision engine will plug into any Java application gatekeeper, and will return granted or denied decisions when asked if a user can access a target with a given command and set of parameters. Users are allocated roles, which are placed in X.509 ACs, signed and stored in an LDAP directory, by the Privilege Allocator (PA). The decision engine will retrieve the user's roles and make decisions based on them, according to an XML authorization policy set by the target's administrator (the Source of Authority or SOA). The policy is also placed in an X.509 AC, and signed and stored in an LDAP directory by the PA.Home Site: http://sec.isi.salford.ac.uk/permis/</p>
<p>Pre-requisites:</p>	<p>Sites will need to either be running a PKI, or have PKI experience, as the site's Source of Authority (SOA) will need to digitally sign the X.509 ACs that are issued to its users. Users do not need to be PKI aware, as PERMIS will allow any type of authentication to take place.</p> <p>Sites should be running an LDAP directory, as the simplest configuration (and easiest to use by the users) is for the X.509 ACs to be stored in the local LDAP directory and fetched from there by the PERMIS decision engine, so that the users do not need to be aware of the ACs (this is called the pull model).</p> <p>Sites will need to have a competent Java programmer, in order to interface the PERMIS decision engine to their Java gatekeeper application.</p> <p>Sites who are running an Entrust PKI, will need to use Java SDK 1.3 until Entrust enables its toolkit to run with Java SDK 1.4.</p> <p>Sites should be familiar with writing XML, as their target authorization policy must be written in XML. The IBM tool XEENA will help them to create syntactically correct policies based on the PERMIS DTD. The PERMIS support team at the University of Salford will also give advice on the creation of semantically correct XML policies.</p> <p>The following supporting tools will also be useful:</p> <p>i) IBM's Xeena, available from http://www.alphaworks.ibm.com/tech/xeena . This will read in the PERMIS DTD, and make sure that your policies are syntactically correct.</p> <p>ii) BER Viewer by Aram Perez provides you with a simple Windows tool to view the ACs that you have created with the PERMIS PA</p>
<p>Deadline:</p>	<p>August 25, 2003.</p>
<p>Evaluation & Reporting:</p>	<p><i>Level 1</i></p> <ol style="list-style-type: none"> 1. Verify installation procedures and the documentation for PERMIS as provided in the Java API Cookbook and the PA Cookbook. <p><i>Level 2:</i></p> <ol style="list-style-type: none"> 1. Demonstrate the capability of system integrators to incorporate the PERMIS API into a fully functioning application gatekeeper. 2. Demonstrate the ability of system administrators (SOAs) to write an effective PERMIS authorization policy, and to allocate the correct X.509 ACs to their users. <p><i>Level 3:</i></p> <ol style="list-style-type: none"> 1. Operational testing of the PERMIS API to ensure that <ol style="list-style-type: none"> i) it is reliable

- ii) it performs well
- iii) it makes correct decisions

Level 4:

1. Inter-institutional operation. Verify that multiple SOAs at multiple sites can authorize their users to access resources at remote sites. This will entail:
 - i) the sites agreeing which roles each will allocate to its users
 - ii) SOAs at each site allocating the appropriate roles to their own users
 - iii) SOAs at target sites setting an appropriate authorization policy for protection of its resources, that grants access to some roles and denies access to others
 - iv) Each site making its LDAP directory available to the PERMIS gatekeeper at the remote sites (so that its roles can be retrieved)

Bug and Enhancement Suggestion reporting mechanisms:

Send bug reports and enhancement suggestions to <nmi-support@nsf-middleware.org> with the subject line: TESTBED-FEEDBACK-PERMIS

If the person who is sending the feedback is not the same as the sender of the email message, indicate name/position of the person who did the evaluation.

Final evaluation report:

Submit an MS-Word format document as an email attachment to: <testbed-reports@sura.org> with a filename in the following format:

Institution_initials-R2-PERMIS.doc

Include the following components in this report –

1. Indication as to the level of testing performed (level 1, 2, 3 or 4) and a list of names/positions of those who participated in the evaluation. Also an indication of the amount of man hours spent on the various tests. If the site was only able to complete partial levels of testing, please provide additional details as to what prohibited testing at higher levels.
2. Listing of date/time/brief summary line of bugs and enhancement suggestions submitted throughout the test cycle. Listing and brief description of any previously undocumented parameters required within the PERMIS configuration.
3. Log (date/time/user/use/result) of all user authorization attempts, and the results returned by the PERMIS PBA API, up to end of test period. *Note that the site is responsible for putting the logging commands into its application gatekeeper.*
4. Listing and brief description of any "best practice" issues associated with this mode of working, as input into NMI dissemination activities.

Support:

Send support requests to <nmi-support@nsf-middleware.org> with the subject line: TESTBED-SUPPORT-PERMIS. Response time is 24 hours or less.

<p>Component:</p> <p><i>New for R3</i></p>	<p>Look - The LDAP operational ORCA "k"ollector</p> <p>Look is a utility written in Perl which gathers LDAP performance data at periodic intervals and generates a file of summary results in a format compatible with the open source ORCA web graphing product (available at <http://www.orcaware.com>). Look is capable of retrieving information from the directory log (currently only iPlanet Directory Server 4.x), as well as querying the LDAP directory directly to retrieve information. Home Site: http://middleware.internet2.edu/dir/</p>
<p>Pre-requisites:</p>	<p>Sites should be running an LDAP directory – either iPlanet Directory Server 4.16 or SunONE Directory Server 5.1.</p> <p>Sites need to be able to run Perl 5.60 and PerLDAP v1.4.1. Future versions of Look will be use NET::LDAP rather than PerLDAP.</p> <p>Sites will require a competent system administrator capable of installing Orca, Look, and Perl if necessary.</p>
<p>Deadline:</p>	<p>August 25, 2003.</p>
<p>Evaluation & Reporting:</p>	<p>Level 1:</p> <ul style="list-style-type: none"> • Verify documentation allows for installation <p>Level 2:</p> <ul style="list-style-type: none"> • Determine whether collected statistics are sufficient. If not, provide suggestions as to additional statistics that are required. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-LOOK.doc</p>
<p>Support:</p>	<p>Send enhancement and support requests to <nmi-support@nsf-middleware.org> with the subject line: TESTBED-SUPPORT-LOOK. Response time is 2 business days or less. Orca listserv available from http://www.orcaware.com.</p>

<p>Component:</p> <p><i>New for R3</i></p>	<p>SAGE - Service for Authorized Group Editing</p> <p>Institutions contemplating projects that require numerous groups to be managed within their enterprise directory services often confront a variety of operational issues to do with the management of, representation of, and access to group information. The creation of a tool to facilitate these operational tasks has been identified as a high priority activity by the Internet2 MACE-Dir working group. Named SAGE, this document is the initial step towards specifying the functional capabilities that it should embody. Home Site: http://middleware.internet2.edu/dir/</p>
<p>Pre-requisites:</p>	<p>Target audience: IT Architects or equivalents; enterprise directory managers and implementers.</p>
<p>Deadline:</p>	<p>August 25, 2003.</p>
<p>Evaluation & Reporting:</p>	<p>Level 1: Review the document and comment on the following:</p> <ol style="list-style-type: none"> a) Is the concept of SAGE clearly communicated? Does the document enable you to form a mental image of what it is that is to be built? b) Is the concept of SAGE a good one, i.e., is it likely to add significant value sooner or later to your institution's core middleware infrastructure? c) Are there additional scenarios that you feel ought to be supported by SAGE? Are there any in the doc that you feel ought to be excluded from further consideration or significantly recast? d) Which means of potential SAGE interaction are likely to be of most use at your site: batch import/export, web services interface, C code library, Perl code library, java code library, other language code library (and please specify which language)? e) Using the terminology of section 3 in the document, which specific consumer technologies do you believe ought to be supported soonest? f) Is this document written at an appropriate level for the target audience? If not, explain why. g) Is this document useful to you? Explain why or why not. h) Do you have any other suggested changes and/or additions? i) Is this document ready for wide publication? Please explain why or why not. j) Indicate your recommended publication and dissemination venues for this document. k) Are you using groups in your enterprise directory service? If yes, how are you managing their administration? What is your rough estimate of the number of groups that will eventually be managed at your site and of the number of independent sources of information (including individual humans) that will determine group information? Also please indicate the rough number of people at your site. <p>As bug or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-SAGE.doc</p>

Support:

Send enhancement and support requests to <nmi-support@nsf-middleware.org> with the subject line:
TESTBED-SUPPORT-SAGE.

Component:	Enterprise Directory Implementation Roadmap
<i>New for R3</i>	The Enterprise Directory Implementation Roadmap is a web-based structure of documentation and related resources that institutions can draw on to help deploy and use NMI-released tools and components pertaining to enterprise directories. Home Site: http://middleware.internet2.edu/dir/
Pre-requisites:	Target audience: Technical and Technology and Project Management staff new to the subject of enterprise directories
Deadline:	August 25, 2003.
Evaluation & Reporting:	<p>a) Review the Web interface and general appearance and comment on the following: Are all the click-able links valid? Is the information presented in an intuitive manner? Does the Roadmap function similarly with different browser versions and vendors?</p> <p>b) Review the Roadmap and comment on the following:</p> <ol style="list-style-type: none"> Does it present the overall issues and steps critical to implementing an enterprise directory? Do you have any suggested changes and/or additions? Does the content of this Roadmap vary widely from your or your institution's experience with enterprise directory services? If yes, please include a write-up on your experience. Would this Roadmap be useful to sites with little or no experience in implementing directory services? Explain why or why not. Is this document written at an appropriate level for the target audience? If not, explain why. Is this Roadmap useful for creating a context for the NMI enterprise directory components? Is this Roadmap ready for wide publication? Explain why or why not. <p>As bug or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-DirRoadmap.doc</p>
Support:	Send enhancement and support requests to <nmi-support@nsf-middleware.org> with the subject line: TESTBED-SUPPORT-DIR-ROADMAP.

<p>Component:</p> <p><i>Updated for R3</i></p>	<p>LDAP Analyzer</p> <p>The LDAP Analyzer Service determines the compliance of an LDAP directory server implementation with various object class definitions such as inetOrgPerson, eduPerson, and the Grid Laboratory Universal Environment (GLUE) schema, as well as the recommendations outlined in the LDAP-recipe and other best practice documents. Home Site: http://middleware.internet2.edu/dir</p> <p>Note: Changes from the previous version are noted in the change log which is provided on the release announcement page on the I2 Middleware Web site.</p>
<p>Pre-requisites:</p>	<p>Target audience: Technical - Directory Server Administrators</p>
<p>Deadline:</p>	<p>August 25, 2003.</p>
<p>Evaluation & Reporting:</p>	<p>a) Verify installation procedures and documentation. Note the system specifications for each installation performed.</p> <p>b) Review the Web interface and general appearance and comment on the following: Are all the click-able links valid? Is the information presented in an intuitive manner? Does the analyzer look different with different browser versions and vendors?</p> <p>c) Exercise the functions provided and comment on the following: Given a directory server with a known configuration, are the analyses correct? Does the analyzer behave erratically with different browser versions or vendors (e.g., receive a time out, "hang", etc.)?</p> <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-LDAPAnalyzer.doc</p>
<p>Support:</p>	<p>Send support requests to nmi-support@nsf-middleware.org with subject line starting with: TESTBED-LDAP-ANALYZER-SUPPORT:</p>

<p>Component:</p> <p><i>Updated for R3</i></p>	<p>Shibboleth 1.0</p> <p>Shibboleth is an open-source, standards-based tool providing mechanisms for controlling access to web based resources (even in inter-institution use), while offering options for protecting personal privacy. It consists of origin site software (Handle Server and Attribute Authority) which manages the release of attribute information, and target side software (modules for the Apache web server) which manages user sessions, obtains user attributes, and makes access control decisions. Together, these components provide an inter-institutional access control framework that allows for the preservation of personal privacy. Home Site: http://shibboleth.internet2.edu</p> <p>Note: Changes from the previous version are noted in the change log which is provided in the deploy guides and on the release announcement page on the Shibboleth Web site.</p>
<p>Pre-requisites:</p>	<p>Origin (campus) sites will require common institutional components in place such as an enterprise LDAP or MySQL directory and a WebISO system.</p> <p>Target (resource/content provider) sites will require an Apache web server, and both target and origin can maintain use of other access systems while testing Shibboleth. Installation and configuration require relatively little labor.</p>
<p>Deadline:</p>	<p>August 25, 2003.</p>
<p>Evaluation & Reporting:</p>	<ul style="list-style-type: none"> • Verify installation procedures and documentation. Note the system specifications for each installation performed. • Identify and briefly describe projects or applications at your site that are not currently using Shibboleth but could benefit from doing so, and describe the anticipated benefits of usage. If steps towards usage are planned within the next 6 months, include an estimated timeline for implementation. • Examine and comment on usability issues and suggested improvements; e.g., design of a tool to manage Attribute Release Policies (ARPs) and Attribute Acceptance Policies (AAPs), better error handling, other interface concerns. • Examine and comment on the compatibility of Shibboleth with other types of systems and suggest or contribute new code and plug-ins. • Install and use Shibboleth within projects or applications at your site. For each project or application, describe the frequency and type of usage (specific components used, actions enabled) and the benefits derived. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-Shibboleth.doc</p>
<p>Support:</p>	<p>Send support, bug, and enhancement requests to mace-shib-users@internet2.edu.</p>

Component:	OpenSAML 0.9
<i>Updated for R3</i>	OpenSAML is a set of open-source libraries in Java and C++ which can be used to build, transport, and parse SAML messages. OpenSAML is able to transform the individual information fields that make up a SAML message, build the correct XML representation, and unpack and process the XML before handing it off to a recipient. OpenSAML fully supports the SAML browser/POST profile for web sign-on, and supports the SOAP binding for exchange of attribute queries and attribute assertions. It does not currently support the browser/artifact profile or other SAML messages involving authorization decisions. Home Site: http://www.opensaml.org
Pre-requisites:	OpenSAML will prove most useful to communities that want to exchange attribute information about recognized principles in a standards-based way (e.g. Shibboleth).
Deadline:	August 25, 2003.
Evaluation & Reporting:	<ul style="list-style-type: none"> • Verify installation procedures and documentation. Note the system specifications for each installation performed. • Verify and comment on proper functionality and design of API's. • If applicable, contribute code modifications to support the artifact profile or other assertion formats. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-OpenSAML.doc</p>
Support:	Send support requests to nmi-support@nsf-middleware.org with subject line starting with: TESTBED-OPENSAML-SUPPORT: For technical questions regarding OpenSAML, use the list (mace-opensaml-users@internet2.edu), subscribe at http://archives.internet2.edu/ .

<p>Component:</p> <p><i>Unchanged for R3</i></p>	<p>KX.509 and KCA v1.0 (standalone) v1.0</p> <p>KX.509 and KCA provide a bridge between a Kerberos and PKI infrastructure. These tools enable the PKI-based security infrastructure of the Globus Toolkit to integrate with Kerberos-based authentication implemented at university campuses. KCA 1.0 (Kerberized Certificate Authority) receives a Kerberos ticket and issues a short-term PKI certificate. KX.509 1.0 is the desktop client that issues a request to the KCA and manages the returned certificate. This is the standalone version of the software, also available bundled with the Globus Toolkit. Home Site: http://www.citi.umich.edu/projects/kerb_pki/</p> <p>Note: Changes from the previous version are noted in the change log which is provided on the release announcement page on the KX.509 Web site.</p>
<p>Pre-requisites:</p>	<p>KCA server runs on Solaris/AIX/Linux machines; KX509 client runs under Windows (9x/2000/ME/XP) /Solaris/Linux. Users already get Kerberos IV or V Tickets at login.</p>
<p>Deadline:</p>	<p>August 25, 2003.</p>
<p>Evaluation & Reporting:</p>	<p>A. Verify installation procedures and documentation. Note the system specifications for each installation performed.</p> <p>B. Demonstrate the capability of users to authenticate locally using Kerberos, run KX.509 to make use of their Kerberos tickets to authenticate to KCA and thereby obtain a short-term X.509 certificate which will work with services (ex. Web-server based) that already use X.509 certificates for authentication. For each exercise or project activity, describe the frequency and type of usage and the benefits derived.</p> <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-KCA-KX509(G).doc</p>
<p>Support:</p>	<p>Send support requests to nmi-support@nsf-middleware.org with subject line: TESTBED-SUPPORT-KX509(SA)</p>

Component:	Certificate Profile Maker v1.1
<i>Unchanged for R3</i>	CPM: Certificate Profile Maker is a CGI-program package for making a certificate profile in XML format. It simultaneously produces a sample X.509 certificate in XML format according to the certificate profile. Home Site: http://middleware.internet2.edu/hepki-tag/
Pre-requisites:	<p>Technical requirements: A UNIX system with Apache to host the software (or) use Certificate Profile Maker from the Internet2 PKI development machine, http://pkidev.internet2.edu/cpm/</p> <p>Operational requirements: General knowledge of PKI and more in-depth understanding of X.509 certificates, certificate profiles, and RFC-2459.</p>
Deadline:	
Evaluation & Reporting:	<ul style="list-style-type: none"> • If installing locally, verify installation procedures and documentation. Note the system specifications for each installation performed. • Exercise the capability of users to generate a valid certificate profile. Summarize the frequency and outcome of these attempts. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-CPMaker.doc</p>
Support:	Send support requests to nmi-support@nsf-middleware.org with subject line starting with TESTBED-CPM-SUPPORT:

<p>Component:</p> <p><i>Unchanged for R3</i></p>	<p>Pubcookie v3.0</p> <p>Pubcookie is an example of a "WebISO" package, a system designed to allow users, with standard web browsers, to authenticate to web based services across many web servers, using a standard, typically username/password central authentication service. Pubcookie consists of a standalone login server and modules for common web server platforms like Apache and Microsoft IIS. Together, these components can turn existing authentication services (like Kerberos, LDAP, or NIS) into a solution for single sign-on authentication to websites throughout an institution.</p> <p>Home Site: http://www.pubcookie.org/</p> <p>Note: Changes from the previous version are noted in the change log which is provided on the release announcement page on the Pubcookie Web site.</p>
<p>Pre-requisites:</p>	<p>Pre-existing authentication service (e.g. Kerberos, LDAP, PKI, shadow passwd file) and some expertise with its interfaces.</p> <p>Experience configuring SSL on Apache & Microsoft IIS web servers.</p>
<p>Deadline:</p>	<p>August 25, 2003.</p>
<p>Evaluation & Reporting:</p>	<ul style="list-style-type: none"> • Verify that Pubcookie overview information is sufficient prior to installation. • Verify Pubcookie installation and documentation. Note the system specifications for each installation performed. • Exercise the capability of users to deploy and test Pubcookie login server. Exercise the capability of users to deploy and test Pubcookie application server in communication with test login server. Summarize the frequency and outcome of these attempts. • Exercise the capability of users to use login server's verifier interface with pre-existing campus authentication infrastructure. Summarize the frequency and outcome of these attempts. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-Pubcookie.doc</p>
<p>Support:</p>	<p>Send support requests to nmi-support@nsf-middleware.org with subject line starting with: TESTBED-PUBCOOKIE-SUPPORT:</p>

Component:	eduPerson (200210)
<i>Unchanged for R3</i>	eduPerson contains the inetorgPerson attributes localized to higher ed and research and 8-10 additional attributes for individuals to foster inter-institutional collaborations. Change summary is included in the document. Home Site: http://www.educause.edu/eduperson/
Pre-requisites:	Enterprise LDAP directory and accompanying directory expertise
Deadline:	August 25, 2003.
Evaluation & Reporting:	<p>Note: If you have already evaluated this component at the level of document review, please concentrate your evaluation effort towards additional depth and experience evaluating the objectclass as it is deployed.</p> <ul style="list-style-type: none"> Review the specification document and note any suggested changes/additions/omissions to attribute descriptions. In addition, comment on the following: <ol style="list-style-type: none"> Is the document written at an appropriate level for the target audience? Explain why or why not. Would you use this objectclass in your environment? Explain why or why not. Is this object class ready for wide distribution and deployment? Explain why or why not. If so, what publication and dissemination venues would you recommend for this object class? Install the objectclass and comment on the ease and process of installation and the ease and process of populating data using this objectclass. Perform test queries against the object class and note any issues or problems that arise. (Please include a detailed configuration of your test environment, including HW configuration, LDAP server/version used, any additional information that would be helpful .) Exercise the objectclass with enterprise or research activities and applications. For each, describe the application and its extent (pilot, intra, inter-institutional), the purpose of using the objectclass with the particular application, and the outcome/benefits of use. Document any additional attributes that would be useful for specific applications, including an explanation of the use and requirements for any proposed attribute(s). <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-eduperson.doc</p>
Support:	Send support requests to nmi-support@nsf-middleware.org with subject line starting with: TESTBED-EDUPERSON-SUPPORT:

Component:	eduOrg (200210)
<i>Unchanged for R3</i>	eduOrg contains institutional attributes, including account management policies, security policies, contacts for key services, etc. Change summary is included in the document. Home Site: http://www.educause.edu/eduperson/
Pre-requisites:	Enterprise LDAP directory and accompanying directory expertise
Deadline:	August 25, 2003.
Evaluation & Reporting:	<p>Note: If you have already evaluated this component at the level of document review, please concentrate your evaluation effort towards additional depth and experience evaluating the objectclass as it is deployed.</p> <ul style="list-style-type: none"> Review the specification document and note any suggested changes/additions/omissions to attribute descriptions. In addition, comment on the following: <ol style="list-style-type: none"> Is the document written at an appropriate level for the target audience? Explain why or why not. Would you use this objectclass in your environment? Explain why or why not. Is this object class ready for wide distribution and deployment? Explain why or why not. If so, what publication and dissemination venues would you recommend for this object class? Install the objectclass and comment on the ease and process of installation and the ease and process of populating data using this objectclass. Perform test queries against the object class and note any issues or problems that arise. (Please include a detailed configuration of your test environment, including HW configuration, LDAP server/version used, any additional information that would be helpful .) Exercise the objectclass with enterprise or research activities and applications. For each, describe the application and its extent (pilot, intra, inter-institutional), the purpose of using the objectclass with the particular application, and the outcome/benefits of use. Document any additional attributes that would be useful for specific applications, including an explanation of the use and requirements for any proposed attribute(s). <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-eduorg.doc</p>
Support:	Send support requests to nmi-support@nsf-middleware.org with subject line starting with: TESTBED-EDUORG-SUPPORT:

<p>Component:</p> <p><i>Unchanged for R3</i></p>	<p>commObject, October 2002</p> <p>commObject is a schema for representing video and voice over IP conferencing endpoints in LDAP directories, enabling portal searching, white pages, and centralized user management. This schema was originally produced by the NMI community and included in NMI release 1. Since that time, the architecture has been improved and submitted to the International Telecommunications Union Standardization Sector (ITU-T) Study Group 16 as a proposed international standard. The NMI community is invited to submit their comments and suggestions on the draft to Study Group 16 for inclusion in the ratification process. Additional advanced implementation scenarios have been added which will be useful to institutions deploying commObject. Home Site: http://middleware.internet2.edu/video/</p>
<p>Pre-requisites:</p>	<p>Enterprise LDAP Directory and accompanying directory expertise. Since these object classes represent h.323 video/voice conferencing endpoints, it is useful to test the classes using real h.323 account and user data.</p>
<p>Deadline:</p>	<p>August 25, 2003.</p>
<p>Evaluation & Reporting:</p>	<p>Note: If you have already evaluated this component at the level of document review, please concentrate your evaluation effort towards additional depth and experience evaluating the objectclass as it is deployed.</p> <ul style="list-style-type: none"> • Review the specification document and note any suggested changes/additions/omissions to attribute descriptions. In addition, comment on the following: <ul style="list-style-type: none"> a) Is the document written at an appropriate level for the target audience? Explain why or why not. b) Would you use this objectclass in your environment? Explain why or why not. c) Is this object class ready for wide distribution and deployment? Explain why or why not. If so, what publication and dissemination venues would you recommend for this object class? • Install the objectclass and comment on the ease and process of installation and the ease and process of populating data using this objectclass. • Perform test queries against the object class and note any issues or problems that arise. (Please include a detailed configuration of your test environment, including HW configuration, LDAP server/version used, any additional information that would be helpful .) • Exercise the objectclass with enterprise or research activities and applications. For each, describe the application and its extent (pilot, intra, inter-institutional), the purpose of using the objectclass with the particular application, and the outcome/benefits of use. Document any additional attributes that would be useful for specific applications, including an explanation of the use and requirements for any proposed attribute(s). <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-commobject.doc</p>

Support:

Send support questions to nmi-support@nsf-middleware.org with subject line starting with:
TESTBED-COMMOBJECT-SUPPORT:

Component:	Certificate Profile Registry
<i>Unchanged for R3</i>	Consists of a profile registry, to hold profiles for standard certificate formats for the community and an institutional root certificate service, to provide a functional way for certificate path construction to be done within the community. Home Site: http://middleware.internet2.edu/certprofiles/
Pre-requisites:	Target audience: Campus security managers & campus PKI implementers
Deadline:	August 25, 2003.
Evaluation & Reporting:	<ul style="list-style-type: none"> • Comment on the sufficiency of the certificate profile formats available in registry. • Comment on the ease of use of submission of profiles and retrieval of profiles from other schools. • Should the registry also include guidance or suggestions for implementers? If so, please note any specific recommendations for topics or resources to include or reference. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-CPregistry.doc</p>
Support:	N/A

Component:	Practices in Directory Groups, October 2002
<i>Unchanged for R3</i>	Experiments and early experiences with facilitation of authorization in applications and facilitation of group messaging with use of directory services in institutions of higher education were surveyed. Several concepts, good practices, open issues, and a few principles extracted from this are presented. Home Site: http://middleware.internet2.edu/dir/
Pre-requisites:	Target audience: IT Architects or equivalents; enterprise directory managers and implementers.
Deadline:	August 25, 2003.
Evaluation & Reporting:	<p>1. Review the document and comment on the following:</p> <ol style="list-style-type: none"> Is this document written at an appropriate level for the target audience? If not, explain why. Is this document useful to you? Explain why or why not. Do you have any suggested changes and/or additions? Does the content of this document vary widely from your or your institution's experience with enterprise directory groups? If yes, please include a write-up on your experience. Is this document ready for wide publication? Explain why or why not. Indicate your recommended publication and dissemination venues for this document. Are you using groups in your enterprise directory? If yes, for what purposes? Highlight uses that are not mentioned in the document. <p>2. Implement services following the specifications in the document. Briefly describe each service, including the extent of the service (pilot, intra- inter-institutional) and the purpose and outcome of using groups as part of the service.</p> <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-Practices-Groups.doc</p>
Support:	N/A

Component:	LDAP Recipe, October 2002
<i>Unchanged for R3</i>	This document is intended to be a discussion point toward the development of common directory deployments within the Higher Education community. In particular, a hope is to have institutions configure and populate their directories in similar ways to enable federated administration and distribution of directory data that allows applications, both client and server, to utilize directory infrastructures. Practical techniques are described and associated with other developments of the NMI such as metadirectories and group management. Change summary is included in the document. Home Site: http://middleware.internet2.edu/dir/
Pre-requisites:	Target audience: IT Architects or equivalents; enterprise directory managers and implementers.
Deadline:	August 25, 2003.
Evaluation & Reporting:	<p>1. Review the document and comment on the following:</p> <ul style="list-style-type: none"> a) Is this document written at an appropriate level for the target audience? If not, explain why. b) Is this document useful to you? Explain why or why not. c) Do you have any suggested changes and/or additions? d) Does the content of this document vary widely from your or your institution's experience with enterprise directory services? If yes, please include a write-up on your experience. e) Is this document ready for wide publication? Explain why or why not. f) Indicate your recommended publication and dissemination venues for this document. g) Are you using groups in your enterprise directory? If yes, for what purposes? h) Highlight uses that are not mentioned in the document. <p>2. Implement a service following the specifications in the document. Briefly describe your implementation experience, including the intended purpose, extent of the service (pilot, intra-, inter-institutional), overall process, timeline, and outcome(s).</p> <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-LDAP-recipe.doc</p>
Support:	N/A

<p>Component:</p> <p><i>Unchanged for R3</i></p>	<p>Metadirectory Practices for Enterprise Directories in Higher Education, October 2002</p> <p>This document offers recommendations to the person or persons at institutions embarking on the implementation of groups. These recommendations are intended to be independent of the actual repository of the group information: LDAP directory, relational database, etc. Where possible, references are made to implementation-specific documentation. Change summary is included in the document. Home Site: http://middleware.internet2.edu/dir/</p>
<p>Pre-requisites:</p>	<p>Target audience: IT Architects or equivalents; enterprise directory managers and implementers.</p>
<p>Deadline:</p>	<p>August 25, 2003.</p>
<p>Evaluation & Reporting:</p>	<ol style="list-style-type: none"> 1. Review the document and comment on the following: <ol style="list-style-type: none"> a) Is this document written at an appropriate level for the target audience? If not, explain why. b) Is this document useful to you? Explain why or why not. c) Do you have any suggested changes and/or additions? d) Does the content of this document vary widely from your or your institution's metadirectory architecture and practices? If yes, please include a write-up on your experience. e) Is this document ready for wide publication? Explain why or why not. f) your recommended publication and dissemination venues for this document. g) Are you using groups in your enterprise directory? If yes, for what purposes? h) Highlight uses that are not mentioned in the document. 2. Implement a service following the specifications in the document. Briefly describe your implementation experience, including the intended purpose, extent of the service (pilot, intra-, inter-institutional), overall process, timeline, and outcome(s). <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-Metadirectory.doc</p>
<p>Support:</p>	<p>N/A</p>

Component:	Shibboleth Architecture v.5, May 2002
<i>Unchanged for R3</i>	Shibboleth, an Internet2/MACE project, is developing architectures, frameworks, and practical technologies to support inter-institutional sharing of resources that are subject to access controls. This paper presents the Shibboleth architecture for the secure exchange of interoperable authorization information that can be used in access control decision-making. The paper will present a high-level view of the interaction between sites and will provide a detailed behavioral description of model components and message exchange formats and protocols. One difference between Shibboleth and other efforts in the access control arena is Shibboleth's emphasis on user privacy and control over information release. Home Site: http://shibboleth.internet2.edu/
Pre-requisites:	Target audience: CIOs and technical management (sections 1 through 4 only), IT Architects or equivalents, and implementers.
Deadline:	August 25, 2003.
Evaluation & Reporting:	<p>1. Review the document and comment on the following from each of the perspectives within the target audience (management, architects, and implementers):</p> <ol style="list-style-type: none"> Is this document written at an appropriate level for the target audience? If not, explain why. Is this document useful to you? Explain why or why not. Do you have any suggested changes and/or additions? Is this document ready for wide publication? Explain why or why not. Indicate your recommended publication and dissemination venues for this document. <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-Shib-architecture.doc</p>
Support:	N/A

<p>Component:</p> <p><i>Unchanged for R3</i></p>	<p>Higher Education PKI (HEPKI) Model Campus Certificate Policy</p> <p>A Certificate Policy (CP) statement defines the terms and conditions under which a campus Certificate Authority (CA) must operate. This document proposes a model CP for use at an institution of Higher Education in the United States. Additionally, as a national infrastructure for PKI matures, it is the intent that this model CP be interoperable with other PKI implementations. This model CP is suitable for use with the Higher Education Bridge Certification Authority (HEBCA). Home Site: http://middleware.internet2.edu/certpolicies/</p>
<p>Pre-requisites:</p>	<p>Target audience: IT Architects or equivalents, campus security managers, campus legal, campus PKI implementers.</p>
<p>Deadline:</p>	<p>August 25, 2003.</p>
<p>Evaluation & Reporting:</p>	<ol style="list-style-type: none"> 1. Review the document and comment on the following: <ol style="list-style-type: none"> a) Is this document written at an appropriate level for the target audience? If not, explain why. b) Is this document useful to you? Explain why or why not. c) Do you have any suggested changes and/or additions? d) Does the content of this document vary widely from your or your institution's experience with campus certificates? If yes, please include a write-up on your experience. e) Is this document ready for wide publication? Explain why or why not. f) Indicate your recommended publication and dissemination venues for this document. g) Are you using groups in your enterprise directory? If yes, for what purposes? h) Highlight uses that are not mentioned in the document. 2. Implement a service following the specifications in the document. Briefly describe your implementation experience, including the intended purpose, extent of the service (pilot, intra-, inter-institutional), overall process, timeline, and outcome(s). <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-HEPKI-policy.doc</p>
<p>Support:</p>	<p>N/A</p>

Component:	Lightweight Campus Certificate Policy and Practice, April 2002
<i>Unchanged for R3</i>	PKI-Lite focuses on employing PKI technology for standard assurance applications that already have established and implemented requirements for initial user authentication and overall system security. Home Site: http://middleware.internet2.edu/hepki-tag/
Pre-requisites:	Target audience: IT Architects or equivalents, campus security managers, campus legal, campus PKI implementers.
Deadline:	August 25, 2003.
Evaluation & Reporting:	<p>1. Review the document and comment on the following:</p> <ol style="list-style-type: none"> Is this document written at an appropriate level for the target audience? If not, explain why. Is this document useful to you? Explain why or why not. Do you have any suggested changes and/or additions? Does the content of this document vary widely from your or your institution's experience with campus certificates? If yes, please include a write-up on your experience. Is this document ready for wide publication? Explain why or why not. Indicate your recommended publication and dissemination venues for this document. Are you using groups in your enterprise directory? If yes, for what purposes? Highlight uses that are not mentioned in the document. <p>2. Implement a service following the specifications in the document. Briefly describe your implementation experience, including the intended purpose, extent of the service (pilot, intra-, inter-institutional), overall process, timeline, and outcome(s).</p> <p>As bugs or enhancement suggestions are identified throughout the evaluation period, report these <u>as they are discovered</u> to nmi-support@nsf-middleware.org, structuring the subject line of the message as:</p> <p>Testbed [component name] [short problem description]</p> <p>Keep a summary list of all bug/enhancement reports (time/date of submission, resolution) for submission with your final evaluation report.</p> <p>Final evaluation report: Submit the above to testbed-reports@sura.org in an MS-Word document with a filename in the following format:</p> <p>Institution_initials-R3-HEPKI-policy.doc</p>
Support:	N/A