Middleware: Addressing the Top IT Issues on Campus

Campus middleware infrastructures are critical strategic resources for addressing cost, security, and access requirements of electronic applications

By **Ann West**

Higher education has traditionally hosted an open and transitory environment, offering services to such diverse communities as the general public and the corporate sector. Individuals enter and leave our institutions at will, and yet we maintain formal and not-so-formal affiliations with them, be they students who are now alumni, parents who are now donors, or conference attendees who are now research collaborators.

In making daily decisions and planning for the future, we can only afford to implement technologies that are worth the effort and support of our valuable staff and useful to our constituents. Ideally, each project would also address more than one critical issue at a time. The middleware common denominators of identity management, authentication and authorization, and information lookup services address many of our top IT issues to varying degrees.

What Is Middleware?

The term middleware refers to an infrastructure that manages security, access, and information exchange on behalf of applications to make it easier for people to collaborate and do their work. In today's Internet, each application provides these functions, using vendor-specific technologies. However, the Enterprise and Desktop Integration Technologies (EDIT) Consortium, part of the National Science Foundation Middleware Initiative (NMI), advocates the enterprise deployment of a collection of vendor-neutral standards to support the core middleware functions of identity management, authentication, authorization, and information lookup.

Identity Management

An identifier is a unique string of characters mapped to a person or service in a particular context. In traditional network-based computing, each time a student was granted access to a new online service, that student was given a new identifier. For example, a person may have an e-mail address, a library ID, a hidden identifier in the system of record, a network ID, and others.

With enterprise middleware, the goal is to establish the relationship among identifiers from various systems (library, administrative, e-mail, and so on) so that information associated with each can be integrated, such as a person's library ID (and number of overdue books) with his or her e-mail address and voicemail box. Typically, institutions assign one unique identifier to each person, and all other identifiers are cross-mapped to it. Identity management in this sense becomes even more critical when campuses begin to share a wide array of resources — what identifiers or related information do you exchange with another campus to allow a graduate student to access a restricted genetics database? Understanding campus identifiers, their characteristics, and the policies that govern their use is critical to moving to the next step.

Authentication Services

Authentication is the process of verifying that the electronic identifier can be reliably mapped to the person using it. Authentication can take a number of forms and uses one or more of the following:

- Something you know, like a password or other shared information
- Something you have, such as a smartcard with a public-key certificate
- Something you are, as evidenced by a retinal scan, fingerprint, or photo

Implementing campus authentication services can reduce the apparent complexity for our constituents and applications: the user has fewer passwords or access technologies, such as digital certificates, and the service plugs into the existing system without the requirement of providing a separate infrastructure. Authentication deployment is a mixture of policy, technology, campus culture, and risk assessment, however: all methodologies are not created equal, and each institutional project team must weigh the parts before developing a plan.

Authorization Services

As noted on the Internet2 Web site,[1] "...authorization indicates what an identified individual or service, properly authenticated, is permitted to do with a networked object or resource." Once the authorization information is associated with the identifier and the corresponding individual is authenticated, the person can access the available

resources and services, such as a restricted clean room, library reserve, computer account, and so on. This is how automatic provisioning, or providing users with their appropriate service mix, is done (or undone).

Once you have determined that a person should be allowed to use a service, you also need to manage the life cycle of that user's access. The person might be noted initially as a junior high basketball camp participant, added later as a political science student, graduated to being an alumni, and moved to the donor list. Your campus' middleware service architecture should be mindful of the institutional environment constraints and needs, technology alternatives, and research efforts in the communities in which you would like to participate.

Information Lookup: Enterprise Directory Services

Enterprise directory services are the key pieces of middleware. The directory itself is a specialized database tuned for fast look-ups by applications and users. The data stored include a person's unique identifier mapped to her system-dependent identifiers, along with related authentication and authorization information. Examples include e-mail address and aliases, phone number, office location, Social Security number, photo, job title, and system access permissions. This interdependent relationship among directories, authentication system, authorization information, and applications requires a coordinated development of middleware services and the services middleware supports.

So what is core enterprise middleware? For the purposes of this article, it is the electronic association of an individual with a unique identifier within a specific context. Associated with this

Beginning Resources List

The Enterprise and Desktop Integration Technologies (EDIT) Consortium, part of the NSF Middleware Initiative (NMI), consists of Internet2, EDUCAUSE, and the Southeastern Universities Research Association (SURA). The following resources are located on the NMI-EDIT Web site <http://www.nmi-edit.org/>. New or update resources are being released every six months. Check the NMI-EDIT site in the spring for additional documents, services, and object classes.

Educational Opportunities: Single- and Multi-Day Workshops
- NMI-EDIT offers half-day and full-day workshops on implementing enterprise middleware targeting CIOs, technical architects, and project managers, covering basic and advanced topics in middleware. They occur at EDUCAUSE annual and regional meetings, Internet2 meetings, and as announced.
- For additional information and networking opportunities with experienced architects and management, consider attending the Campus Architectural Middleware Planning (CAMP) sessions to be held in Tempe, Arizona, February 5–7, 2003, and Boulder, Colorado, June and July, 2003. Check the NMI-EDIT Web site for details.

Getting Started: Business Case and Practice Documents
- Sample Middleware Business Case: Provides help in convincing decision makers at your institution to commit resources to middleware deployments.
- Middleware Business Case: The Writer's Guide provides suggestions for customizing the Business Case to meet institution-specific needs.
- Identifiers, Authentication, and Directories: Best Practices

for Higher Education offers current practices in these important areas of middleware.
- Template and Sample Campus Identifier Mappings: Offers case studies of identifier surveys from several campuses. Presented in table form, the mappings include characteristics of and assignment information for the institutions' various identifiers. Also included is a sample template.

Enterprise Directories: Practice Documents, Object Classes, and Services
- LDAP Recipe: Includes recommended ways to populate directories within the higher education community.
- Practices in Directory Groups: Includes concepts, good practices, open issues, and principles resulting from early experiences with authorization and group messaging using directory services at higher education institutions.
- Metadirectory Practices for the Enterprise Directory in Higher Education: Offers alternative approaches to the metadirectory functions of information flow, transformation, and redistribution.
- eduPerson Object Class: Contains the inetOrgPerson attributes localized to higher education and research, as well as additional attributes to foster inter-institutional collaborations.
- eduOrg Object Class: Associates attributes to institutions, such as management and security policies, and can be used to discern the organizational structure of a college, for example.
- LDAP Analyzer Service: Determines the compliance of an LDAP directory server implementation with specific object class definitions, such as inetOrgPerson and eduPerson, as well as the recommendations outlined in the LDAP Recipe and other best-practice documents.

unique identifier is information about the individual that can be used for authentication (determining what unique identifier is mapped to that person) and authorization (what the person associated to that identifier can do).

What's the Problem? The Top Ten IT Issues

To discern how middleware can help requires first deciding what the problems are. I wanted a list that was common to a wide variety of campuses, so I turned to this year's EDUCAUSE top 10 IT issues[2] as highlighted in *EDUCAUSE Quarterly*. Participants taking the EDUCAUSE Current Issues Survey were asked to pick their top five issues based on their answers to four questions:

1. Which of the IT-related issues below are most important for your campus to resolve for its strategic success?
2. Which of the IT-related issues below have the potential to become much more significant in the coming year?
3. Which of the IT-related issues below are you as an IT leader or administrator spending most of your time addressing?
4. On which of the IT-related issues below is your campus spending the most human and/or financial resources?

From the results of this survey, 10 issues were picked as being significant answers to at least three of the questions. Portals, although not in the top 10, were included as a special mention in the article because they have the potential of becoming much more significant in the next year. The top 10 issues included

- Administrative Systems/ERP
- IT Funding Strategies
- Faculty Development, Support, and Training
- IT Strategic Planning
- Security Management
- Online Student Services
- Teaching and Learning Strategies
- Distance Education
- Maintaining Network Infrastructure
- Emerging Network Technologies
- (Portals)

On each item on this formidable list, middleware has either a direct or indirect impact. To make this clearer, let's look at the commonalities among them.

How Can Middleware Help?

Most of these issues are related to online services campuses either offer or would like to offer to faculty, staff, and other constituencies. Some of them relate to infrastructure, and two of them relate directly to planning. Despite the seeming discontinuity, a number of threads weave throughout that middleware addresses directly.

Money and Time

IT organizations are being asked to do more with the same or fewer resources. Lists of potential projects in IT are getting longer and more complex. How are we to deploy tailored services for new-student recruiting, on the one hand, and have the incoming freshmen added to the course management system for their orientation, on the other?

- Middleware provides a centralized way of managing access to a wide range of online services. The alternative is to grant access to each service separately, requiring new access, account infrastructure, and staff time for each application offered. However, if these separate infrastructures are consolidated using middleware, the same number of staff can manage a larger suite of services and realize significant time savings during application deployment.

Integration of Services

Given the increased demand for integrated services, such as administrative and academic portals, we need to leverage our telecommunications, facilities, network, application, academic, and administration data.

- Accommodating remote and home workers through the electronic management of their access points is cost effective and a smart human resources policy. This could take the form of a Web page with voice, fax, e-mail, and pager numbers, with the capability of forwarding incoming calls or messages from one or all to another loca-

tion or another person for a specified period of time. Integration of access points and appropriate verification of identity is critical for implementing these types of services.
- Facilitating integrated services can also mean setting up an electronic trust relationship with another organization. For instance, a faculty member signs in to her college portal page, clicks on the financial services logo, calculates her annuities withholdings for the year, and updates her retirement and allocation, without providing additional retirement, salary, or authentication information.

Technical Expression of Business Requirements and Rules

We need to ensure that the access to our electronic resources is according to institutional legal, policy, and funding parameters. This applies to future inter-institutional services in addition to on-campus ones.

- The Family Educational Rights and Privacy Act legislates the statement and use of directory information. Future legislation probably will further underscore our responsibility as stewards and not owners of our constituents' data. To mitigate our risk, we need a good model of our data, how it is used and for what purposes, and the ability to alter what users can access. This is most efficiently done through the consolidation of access and provisioning.
- Administrative business changes can be reflected in academic systems and vice versa. For instance, if a student is accused of plagiarism for a third time, that student's access to the library, computer accounts, student health facilities, and academic labs can be electronically frozen until the issue is decided.

Enhanced Security

Many types of online services, including operating systems, Web services, remote access, and enterprise applications, can be integrated using directory services. Once done, the task of managing user access to them is reduced to just one place — the middleware.

- Because access to computer accounts is governed by the enterprise directory, once a student graduates, his status in the institution's system of record is updated and reflected in the directory. This directory status change causes his computer account in the academic department to be deactivated. Using this method to provision accounts reduces the amount of work needed to disable old ones and the risks associated with nonaffiliated individuals having access to your resources.
- Because the same user credential is presented to all integrated services, all system and application log files reference the same identifier. This greatly enhances auditing of online activity, allowing more complete investigations of alleged cases of abuse and increasing institutional due diligence, thereby reducing liability.

Ease of Use

Improving the use of our systems — by providing single sign-on, for example — helps ensure that faculty, staff, and students benefit from online services. Coupling this with a common directory enables users to specify preferences that personalize applications and enhance or streamline their online experience.

- A faculty member can have his class roster in the course management system updated automatically with the added/dropped students, along with their photos so that he can address them by name on their first day in class.
- Users who forget their passwords can provide private directory information on a password reset page and soon be back working without calling the help desk.
- Students can update their personal information as it changes without visiting the financial aid, registrar, and athletics offices.

Capability to Iterate and Deploy Faster

In developing new services, we sometimes need to adjust our implementations midstream. Having a middleware infrastructure significantly reduces the overhead for deployment and the subsequent tweaking usually required.

- In setting up a purchased wireless service, IT can use the established campus authentication system to ensure a student's identity and track her eligibility (for example, has she paid her bill?) in the directory.
- One group of staff members is responsible for implementing the institution's business rules.
- New services can be deployed faster because the staff doesn't need to set up another database to govern access.
- Authorization changes, such as enabling another group to use a service, can be made quickly.

Privacy

Strategically, it makes sense to be mindful of our constituents' privacy. Sharing precious resources among institutions requires maintaining large access lists of constituents unless we can exchange authorization information.

- A forestry graduate student wants to access a restricted research database that only forestry researchers are allowed to use. She makes no prior arrangements, but is allowed access because her institution electronically vouched for her authenticity as a researcher in that field. She also knows her campus didn't give out her name or e-mail address, because she electronically set up a restrictive, personal-information release policy.

Beginning a Middleware Implementation

Once a campus has committed to deploying this infrastructure, there are no fail-safe, detailed steps it can follow when implementing these technologies. The best you can do is adopt recommended approaches, understanding that "mileage may vary." Each campus has a unique culture, policy structure, and technology environment that inform its middleware implementation. In addition to a technological infrastructure, typical outcomes of this deployment include developing new administrative policies and processes to let online applications and security systems access and use institutional data.

The good news is that campuses have at their disposal a growing set of middleware resources and educational opportunities. Some basic steps toward implementing an enterprise directory service follow:

- *Develop a campus business case and discuss needs with campus stakeholders.* Start by reviewing the "Sample Business Case" for middleware and consider how it could apply to your own institutional drivers. Begin discussing with your staff and project stakeholders how IT can accommodate technology service needs on campus. Attend one of the workshops offered by the National Science Foundation (NSF) Middleware Initiative, NMI (see the sidebar on resources).

- *Inventory your campus identifiers, noting how they are assigned, by whom, and to whom.* Take an inventory of your campus identifiers, such as those used by the campus card, library, administrative, and e-mail systems. Research how people are assigned those identifiers and what services are accessed using them. Develop a system for assigning a unique identifier as a root for cross correlation.

- *Review application and directory requirements.* Build the campus' enterprise directory services next. Begin by reviewing your institutional, technical, and application requirements and needs. Review vendor implementations of enterprise directories. Review the documents available, such as the LDAP Recipe and the eduPerson object class. Consider both on-campus needs and future inter-institutional applications. Continue your education process with stakeholders, move on to the campus data custodians, and begin identifying business-driven applications that would benefit from using a directory.

- *Design and populate your directory.* Set up your schema and identify the data sources. Work with the data custodians, and make sure you understand the definitions of your data. For example, in the

student system, how does an admitted student become a full-time student allowed to use resources? At this point, review and design a mechanism to reconcile identifiers from the various data sources and map them to the campus' unique identifier. This permits consolidating under one entry a person's directory information from disparate sources. Develop a process to populate your directory. Once ready for testing, use the LDAP Analyzer tool to ensure that your directory conforms to the eduPerson object class definition and related good practices.

■ *Deploy the directory and targeted application.*
Start small. Success in a limited area with a visible, needed application will go a long way in convincing the campus community of the project's benefits. Overprovision your service to ensure good performance. Again, check your implementation process by sending your technical staff to an NMI workshop and start them networking with experienced middleware architects.

These are by no means all the steps required to implement enterprise directory services, the linchpin of your middleware infrastructure — but they are the major ones. Keeping tabs on what's happening with middleware development and talking with middleware-savvy staff from a school similar to your own can help reduce the "reinventing the wheel" syndrome.

Putting It All Together

IT infrastructures, such as network and administrative systems, are strategic resources that can be leveraged to service needs across the institution. Deploying a middleware infrastructure is no exception. In fact, it allows us to offer tailored, secure, and interactive services in the areas of teaching, research, and recruitment that we cannot afford to offer now. Middleware lets us move forward, broadening our future service possibilities through the centralization of provisioning information and systems — identity, authentication, and authorization —

and assignment of access based on a person's role within the institution. Once these information, process, and technical systems are in place, the effort to quickly add new services, or people, to our service mix is greatly reduced. *e*

Endnotes
1. See <http://middleware.internet2.edu>.
2. P. Kobulnicky, J. A. Rudy, and the EDUCAUSE Current Issues Committee, "Third Annual EDUCAUSE Survey Identifies Current IT Issues," *EDUCAUSE Quarterly*, Vol. 25, No. 2, 2002, pp. 8–21.

Ann West (awest@educause.edu) manages the NMI-EDIT outreach and educational activities under the auspices of the National Science Foundation Middleware Initiative.