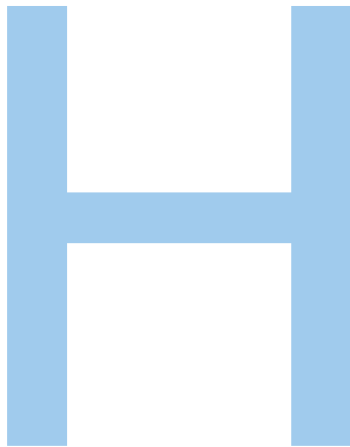




The Middleware C O N N E C T I O N

One of the most important technology infrastructure components emerging today will make possible the high levels of access and collaboration that campus constituents have come to expect.

By Ann West and Maryann Terrana



igher education has traditionally hosted an open and heterogeneous environment, offering services to diverse communities, including the general public and the corporate sector. Individuals often enter and leave our institutions at will, and we maintain formal and causal affiliations with

them—be they applicants, students, alumni, parents who become donors, or conference attendees who become research collaborators.

Coupling this dynamic environment with the growing requirements and desire for electronic collaboration presents a daunting task for any information technology department. To save money, we would like to share library resources among several competitors. To enhance our reputation, we would like to increase our research dollars by facilitating interaction among researchers from different campuses. And to engage our alumni, we would like to offer a suite of online classmate communication and institutional interaction services. Many of these provisions require similar functions and responses to the same questions:

- Are the people who are using these services who they claim to be?
- Are they members of our campus community?
- Do they have permission to use these services?
- Is their privacy being protected?

Addressing the challenges of openness and collaboration is a new technology infrastructure—generically called *enterprise middleware*—that is emerging throughout higher education, government, and other sectors. The term *middleware* refers to a broad infrastructure that, at its core level, manages security, access, and information exchange on behalf of applications to make it easier for people to connect and accomplish their work. The essential components enabling middleware's operation are identity management and authentication, authorization, and directory services. (To help put middleware in context, see the September 2002 issue of *Business Officer*, "Integrating to the Max.")

Middleware provides for the electronic association of an individual with a unique identifier within a specific context. Associated with this unique identifier is information about the individual used for authentication (determining what unique identifier is mapped to that person) and authorization (what the person associated with that identifier has permission to do). Directory services provide the central data repository, tying all services together. As its development continues, mid-

dleware looks to become the glue holding together our collaborative, ubiquitous, and complex systems—enabling the high levels of access and connection that our varied campus constituents have come to expect.

One Student, Many Identities

In traditional network-based computing, each time a student or other system user is granted access to a new online service, that user is given a new identifier. For example, a student may have an e-mail address, a library ID, a hidden identifier in the system of record, a network ID, and so forth. With enterprise middleware, the goal is to establish the relationship among identifiers from various systems (library, administrative, e-mail, etc.), enabling the information associated with each to be integrated. For example, the association of a student's library ID with his or her e-mail address allows the library staff to automatically send e-mail notification of overdue books. Institutions typically assign one unique identifier to each person and cross-map all other identifiers to it.

Identity management becomes even more critical when campuses begin sharing a wide array of resources. For instance, what identifiers or related information should you exchange with another campus to allow one of your graduate students to access a restricted genetics database on another campus? Understanding campus identifiers, their characteristics, and the policies that govern their use is critical before moving to the next step—authentication.

A Guarantee of Authenticity

Authentication is the process of verifying that an electronic identifier is correctly mapped to the person using it. Authentication may take a variety of forms and typically relies on one or more of the following:

- something you know, such as a password;
- something you have, such as a smartcard with a public-key certificate;
- some personal attribute, evidenced by a retinal scan, fingerprint, or photo.

Implementing campus authentication services can reduce complexity for constituents and applications. For instance, with an authentication service, a user has fewer passwords to remember, and the service can plug into an existing system without requiring a separate infrastructure. A word of caution: Authentication deployment requires a careful assessment of campus policy, technology, culture, and risk. All methodologies are not created equal, and your institutional project team must weigh the pros and cons of each before developing an authentication plan. Once an authentication plan is in place, the authorization process determines what an individual may access or do electronically. ►

The purpose of middleware is to manage user access to information, software applications, operating systems, and remote systems.

Authorized Users Only

Once authorization information is associated with the identifier and the corresponding person is authenticated, that individual can access all relevant resources and services, such as a restricted clean room, library reserve, or computer account. This is how automatic provisioning—providing users with their appropriate service mix—is granted or denied.

For instance, let's say Mary has been reported to Zenith University's dean of students for plagiarism. The dean searches for Mary's record and places an electronic hold on it. Within five minutes, Mary cannot send or receive e-mail, check out library books, enter the restricted lab, use the student health facility, or access her computer files. After reviewing Mary's case, the dean finds the accusation in error and removes the hold, restoring Mary's access minutes later.

Once you have determined that an individual is allowed access to a service, you must also manage the life cycle of that user's access. For instance, a user who is initially identified as a junior high basketball camper might subsequently hold a series of roles, each of which is independent of the others: political science student, graduate, and donor. With each transition, the user's service mix will likely change, on the basis of the evolving interests of the individual and the levels of access to campus services and facilities that are appropriate for each particular stage in the user's "life."

Another example depicts how authorization can remain fluid and be directed remotely by university staff and faculty. John, Zenith University's admissions director, is waiting to board a plane and receives a call informing him that a prominent U.S. senator and his daughter intend to visit campus later that day. Concerned about security, John uses his laptop to connect to ZU's intranet and delegates access of his voice mail and e-mail to his assistant for the next four hours. He then sends a signed, encrypted note to the campus safety director, which notifies her of the senator's visit and contains a draft of the agenda to begin security planning. Without these sophisticated and remote capabilities, John would be ill-equipped to control factors that affect the successful recruitment of a student—in this case, of a senator's daughter.

The purpose of middleware is to manage user access to information, software applications, operating systems, and remote systems. This high level of integration is accomplished by using enterprise directories—specialized databases designed for expedient reference checks by applications and users.

Enterprise Directory Services

Enterprise directory services constitute the backbone of middleware. The data stored include a person's unique identifier—

mapped to his or her system-dependent identifiers—and 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 coordinated development of the services middleware supports.

To illustrate the interplay of all these middleware components, consider the following example: Bill, a prospective Zenith University student, fills out an admissions application available on ZU's Web site and also requests information on academic and recreation topics of interest to him. Two weeks later, Bill receives e-mail from ZU about an upcoming bike race and a women's studies department lecture, as well as a reminder of the financial aid application deadline.

In this example, the identification information Bill supplies in his application is stored centrally, allowing ZU content providers such as student life and the staffs of academic departments to have access. Furthermore, this information is added to the enterprise directory so that various approved applications—not only the portal—can retrieve its contents. In a broader context, information such as this can be used to fulfill the objectives of various departments: admissions may seek to attract a new student; the library can ensure appropriate access to online databases; the IT department can control access to the campus wireless network and related services; and financial staff may deploy e-procurement.

The Momentum Behind Middleware

These days, our lives are a mixture of interrelated and overlapping roles that have dramatically increased our expectations regarding technology. With the wide use and availability of e-mail and cell phones, work and leisure are no longer distinct periods of time. The ease of accessing, purchasing, and working via the Web is catching up to the capability of networks, computer power, and storage. Whereas several years ago most network services were associated with a campus or business, individuals now use commercial Internet services in their homes, e-mail cafés, and libraries, as well as from their cell phones. Not only do we want to read our e-mail, we also want to access our courses, research, and work applications and files from all of these entry points. We're coupling our integrated work and leisure time with an expectation of undiminished access to electronic resources.

At the same time, we want all this to be easy and seamless. We don't want to remember multiple user IDs and passwords

associated with our electronic services, memberships, and affiliations. We also don't want to type in our mailing address every time we purchase a plane ticket or a book online, and so we're happy to have the airline or book distributor store it for us electronically. Substantial questions regarding privacy and security are associated with having our personal information duplicated in multiple resource and service provider databases, and these present a real concern that higher education business officers must address head on. Having said this, many of the top concerns facing the business officer in the age of increased electronic access—cost and security chief among them—are addressed by middleware.

Effectively managing IT costs and demonstrating the value of IT investments are now more expected than ever. Middleware provides a centralized way to manage access to a wide range of online services. Separate infrastructures are no longer needed for each service, including issuing new user accounts or the management of multiple user accounts.

Likewise, by consolidating access-control mechanisms, an increased level of security is achieved, given that one staff supports these critical systems. New services, such as wireless access to networked resources, can be added to the mix more quickly and securely when the identity, authentication, and authorization infrastructure already exists. In addition, institutional privacy policies can be put in place and enforced if the information and service access is consolidated using middleware. Once implemented, middleware allows broader service offerings coupled with appropriate access to those services. It enables without increasing risk, and in many cases it can decrease risk. For instance, eliminating multiple user IDs and passwords means that fewer miscellaneous Post-it notes would be strewn about containing sensi-

tive access information that unauthorized users might be tempted to use.

In another example, a faculty member develops a comprehensive research site, detailing sensitive intellectual property. By not linking it to the department page, she believes that her site is secure. What she may not know is that search engines crawl Web sites to find new links. Before she knows it, her research site might be available for any Internet user to view. Middleware-enabled applications written to help users manage their resources—including Web sites—reinforce security policies and procedures.

In an alternate scenario, the faculty member accesses a management Web page and enters the location of her course site and the e-mail addresses of the research team from the collaborating institutions. The site is restricted within minutes. The participating members can then use their campus user IDs and passwords to authenticate and don't need yet another set of credentials to access the project resources. The faculty member is thereby able to offer more information and servic-

The day is soon coming when technology will offer mass customization, affording large populations services or goods tailored to their individual needs.

es online with less risk to her intellectual property rights, as well as the institution's.

Making Middleware Work

Once a campus has committed to a middleware infrastructure, no fail-safe procedures exist for implementing these technologies. Each college and university campus has a unique culture, policy structure, and technology environment that must inform its specific middleware service architecture and implementation. In addition to a technological infrastructure, typical outcomes of this deployment include developing new administrative policies and processes that let online applications and security systems access and use institutional data.

The good news for business officers is that a growing group of experts is available to assist campuses with implementation, and opportunities exist for learning more about how to proceed. The following steps, initiated early, will position your campus to offer the kind of customization and collaboration capability available with middleware to your full array of institutional communities.

Educate yourself and your campus about emerging middleware trends. Find out how your campus handles functions of identification, authentication, and authorization. Discover whether economies of scale can be realized by putting a mid-

dleware infrastructure in place. As the business officer, make sure you understand the business case for doing so before proceeding to the next step.

Talk to your information technology department. Begin discussing with your CIO or IT staff their plans for supporting middleware. Offer your support. While the campus CIO is a major champion of any middleware project, in some cases, the business officer can make or break a middleware deployment. Money usually isn't the issue; data ownership and its institutional use usually are.

Share and compare your middleware knowledge. Successful middleware deployment requires a strong partnership among the technology, business, and academic constituents of an institution. To strengthen these relationships, find out what your counterparts at other campuses have done and share with them the middleware strategy that is working for you. Use the online community at www.nacubo.org to compare processes, administrative policies, and security issues that arise as you move forward.

The day is soon coming when technology will offer mass customization, affording large populations services or goods tailored to their individual needs. More sophisticated collaboration technologies are being tested—the use of which are spawning increased opportunities for people to communicate virtually. As we move forward with the promise of this customization and collaboration, business officers must understand that the functionality of middleware is built on a foundation of identity, authentication, and authorization. Integrating these within the technology infrastructure of our campuses will be critical for realizing the full potential of opportunities that will soon be available.

Resources

The Enterprise and Desktop Integration Technologies Consortium (EDIT), part of the National Science Foundation's Middleware Initiative (NMI), is working on tools and architectures to advance collaboration and interinstitutional resource sharing in the research and higher education communities. The consortium consists of Internet2, EDUCAUSE, and the Southeastern Universities Research Association. It provides resources and educational opportunities available from its Web site (www.nmi-edit.org) to help campuses deploy or enhance their middleware implementations. Among these resources is a sample middleware business case that campus leaders can compare with their institutional drivers to reveal potential benefits. For more information about the overall NMI project, go to www.nsf-middleware.org.



Ann West

Author Bios Ann West manages the NMI-EDIT outreach activities for EDUCAUSE and Internet2 on a research appointment from Michigan Technological University, Houghton. Maryann Terrana is program manager for business, external affairs, and research at NACUBO.

E-mail awest@educause.edu;
maryann.terrana@nacubo.org



Maryann Terrana