

# Identity and Access Management: Technological Implementation of Policy

- Navigating the multiple processes for accessing ever-multiplying campus information systems can be a daunting task for students, faculty, and staff. This article provides a brief overview of Identity and Access Management Services. The authors review key characteristics and components of this new information architecture and address the issue of why a campus would want to implement these services. Implementation issues, particularly those where technology and policy intersect, are also discussed.

by Jeff von Munkwitz-Smith and Ann West

*Jeff's in his office and the telephone rings. The display gives him the number; it's one he recognizes. "Hi Dave, what can I do for you," he says. Dave is the director of First Year Programs and they speak pretty often. "Hi, Jeff! Some of the students in my Peer Mentoring classes are registered for the wrong sections. What's the best way to fix it?," Dave asks. "Send me a list," he replies. A few minutes later, he receives an e-mail message with a list of students to move to different sections. He gives the list to one of the staff in the Enrollment Services section of his department and a while later can let Dave know that the students are now in the correct sections.*

*Later a student knocks on his door. She's dressed in a suit and she's in tears. "Can you help me? I was in your class a few years ago." She asks. "Sure, Jennifer, I remember you. What do you need?" "I lost my purse and I need a transcript for an internship interview and I can't get a transcript without my ID card, what can I do?" "No problem, I know who you are," he tells her and informs the appropriate staff person that it's ok to give Jennifer her transcript.*

What do these two situations have in common? In both, the transactions depended on the identities of the people involved, Jeff's ability to verify their identities (and his staff members' ability to verify his identity), and the appropriateness of the transactions they requested to their roles.

Clearly, it works on an occasional basis, since we do it all the time. However, it doesn't scale. Many of the nearly two thousand faculty and 26,000 students like their problems solved promptly, but Jeff likes to sleep at night and take the occasional day off!

## Identity and Access Management

Automated approaches to these problems are not new. Access is typically managed differently in each system and then aug-

mented in an *ad hoc* fashion by people like the examples above. This wasn't a big problem years ago, when the number of systems that a person might use was limited. Now, a person might be granted access and authorities for e-mail, voice-mail, the student information system, the human resources system, the financial system, the course management system, the library system, an electronic portfolio, a campus portal, a data warehouse or data mart or two, a local area network, and who-knows-what-other campus resources. All of these might require separate applications for access, customization profiles, and IDs and passwords. Navigating the multiple processes for gaining access can be a daunting task for any new student, employee, or faculty member.

Enter the identity and access management services. This new information infrastructure has several key characteristics.

- It integrates all the pertinent information about people from multiple authoritative source systems such as those listed above. This reconciles the accounts we all have in these systems and joins our identities together under one campus unique identity. Using such a system, an application in the library, for instance, might use a person's library system ID to look up that person's e-mail address, campus address, and role at the institution to generate a message that a recalled book was being sent, print a label to use to send the book through the campus mail system, and verify the person's role at the institution to determine a due date for the book, extracting information from separate systems with separate identifiers.
- It processes and transforms information about people including their affiliations with the institution, employment status, and resource access. It then pushes out and stores the information where it can be of use to applications. For example, a campus advising system resource on study habits and the college transition is only licensed for freshmen on campus. The resource needs class standing

to verify access, but the student information system only stores credit information. This piece of information could be computed and stored in the identity management infrastructure.

And let's say ten applications written by different developers wanted to use this same information. Each of them would need to contact someone regarding the algorithm: How would someone know if they've done it correctly? How would the developers know if there are changes in the computation? Computing class standing once and making it available to applications increases likelihood of data accuracy and security and reduces development time. If the student drops out of school in the middle of the term, his or her class standing changes and access is no longer granted.

- It acts as a focus for implementation of policies concerning visibility and privacy of identity information and entitlement policies across the systems. In many cases, it's difficult to implement a privacy service that allows individuals to set higher levels of privacy in some instances (such as a request from outside the institution) than others. Having a central place for management of identity allows the individual to set a privacy profile based on policy governing the types of information being released and under what conditions. This in turn can be used by application developers across the institution.

### Components of Identity Management

The key components of Identity Management can be summarized by four questions:

- Who are you? (Identification)
- How do we know? (Authentication)
- What services and transactions are available to you? (Authorization)
- Is the information about you secure? (Privacy)

“Identity” is the set of attributes about, and identifiers referring to, an individual. The question “Who are you?” is usually answered by a username or ID that uniquely identifies an individual user. It might be an identifier already associated with an individual, such as the SSN. It might be system-assigned, as is the case with many of our administrative sys-

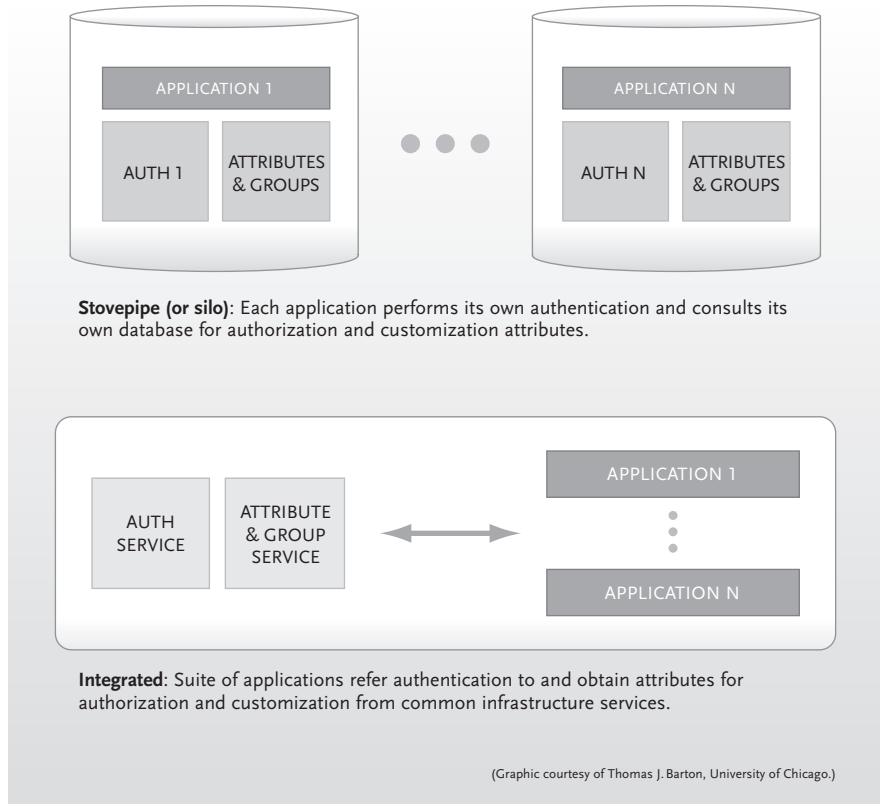


FIGURE 1: COMPARATIVE SERVICE ARCHITECTURES

tems. Or it might be user-assigned, as is the case with most commercial services we access via the Web.

“Authentication” is the process used to verify that individual’s, or “subject’s,” association with an identifier. The most common form of authentication used by our system is a password. Identity cards, often used in combination with a password or personal identification number are also common, particularly with financial transactions. A less common method of authentication, outside of the movies, is biometric identification using a unique physical characteristic, such as a fingerprint, voiceprint, or retinal pattern. The most secure authentication would use a combination of these forms. Identification and authentication link the electronic identity to the physical individual.

“Authorization” is the process of determining if policy permits an intended action to proceed. For individual systems—online library resources, for example—the authorization for access might be all or nothing. For other systems the authorization might be group-based or role-based. An example of this access might be one where all employees have access to view their own payroll information, but only payroll staff are able to update that information. In other cases, the authorization could be controlled at the transaction and field level, with the individual being able to process certain types of transactions for a limited range of data, such as the chair of

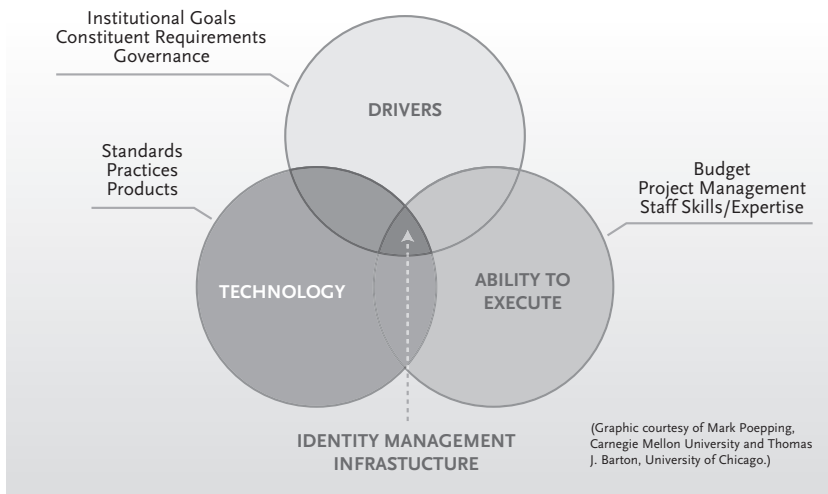


FIGURE 2: IDENTITY MANAGEMENT FACTORS

history department being the only member of that department allowed to update course instructors. Electronic authorization is, ideally, the technical manifestation of institutional policy. Its efficacy is limited by the availability of subject attributes and by how faithfully policy is incorporated in the infrastructure or application.

### Why would your campus want one?

Besides the obvious opportunities for making existing services more convenient to use and for developing new services not easily possible using older systems for authorization and authentication, there are six reasons why an institution ought to consider implementing an identity and access management system.

- **Reduced overhead of service management**—In typical application delivery models, each service maintains its own user identity store and related authentication (and authorization) services. Simplifying the authentication model by having the applications use the same shared identity and access infrastructure not only reduces the staff and resulting overhead required to manage each application, but also achieves substantial economies of scale for the service providers and results in time and system cost savings. Having consolidated systems and business processes for authentication services also reduces the cost and time to deploy new applications. Since these services do not need to be created for each new application, the cost and time of doing so, and the recurring cost of independently maintaining those services are mitigated. (See Figure 1.)
- **Increased security**—Security and privacy issues are not new to higher education. After all, we've operated under FERPA (Family Educational Rights and Privacy Act) since 1974. With the growth of identity theft there is a greater awareness and, as we discuss below, the regulatory requirements have become more stringent. Consolidating the

identity and access services for separate applications means that related policies can be supported in one protected place by the same group of staff. Because the same user credential is presented to all integrated services, all system and application log files reference the same identifier. This enables a consolidated approach to logging which assists in the investigations of alleged cases of abuse. In reduced sign-on instances, users need to remember fewer credentials. They may therefore employ less creative password memory-jogging mechanisms, and are more likely to remember them. For those campuses with a distributed model that provide password feeds to departments to simulate a single-password environment, having the applications instead

access a consolidated authentication service reduces the likelihood of password theft and the chance the department password data is corrupted.

- **Simplified network and online service access**—Consolidated authentication can enable unified identity verification for many online services, so our constituents need only to provide a reduced set of credentials, with user ID/password pairs being the most common. Because of the integration with Web-based applications, solutions to common service issues like self-service password resetting and management are enabled using a common infrastructure.
- **Contractual requirements**—Campuses must be able to prove that resources are being used by the subjects licensed to do so. This could be due to a specific library or course-resource contract or because of funding agency requirements and access to restricted research findings. For example, a faculty member working on a classified project might need to provide funding and employment status—information currently stored in two different administrative systems—for access to online resources. Another illustration includes an e-procurement site that might want information on the employment status, title, and department in order to make a decision to process an individual's order. Contractual obligations, such as those restricting access to licensed electronic resources to people affiliated with our institutions, also play a role. When we charge users fees—either directly or as part of a general student fee—for use of specific resources, such as student recreational facilities, we may want to ensure that only the group that pays has access to those resources.
- **Legal pressures**—Institutions are required to restrict access to health, financial, and academic records. And while FERPA requires us to keep student information private, both the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLB) include requirements that we have plans

## MORE INFORMATION ON IDENTITY AND ACCESS MANAGEMENT SYSTEMS

The NMI-EDIT Consortium (Enterprise and Desktop Integration Technologies–EDIT) Consortium, part of the NSF Middleware Initiative (NMI), comprises Internet2, EDUCAUSE, and the Southeastern Universities Research Association (SURA). The Consortium offers practice documents, software, tools, and architectures to facilitate inter-institutional resources sharing and collaboration. For more information on the components in an identity management system, review the following:

- NMI-EDIT offers half-day and full-day workshops for CIOs, technical architects, and project managers, covering basic and advanced topics in

identity and access management and related topics. Visit the NMI-EDIT Web site at [www.nmi-edit.org](http://www.nmi-edit.org) for locations, topics, and dates.

- For additional information and networking opportunities with experienced architects and management, consider attending the Campus Architectural Middleware Planning (CAMP) sessions. Check the NMI-EDIT, EDUCAUSE, or Internet2 Web sites for details.
- For a current list of tools, documents, software and schemas available from NMI-EDIT relating to identity management components, visit the

Releases section of the NMI-EDIT Web site or the Internet2 Middleware Initiative site at <http://middleware.internet2.edu>.

- To discuss Identity Management with your colleagues, subscribe to the EDUCAUSE Middleware Constituent Group at [www.educause.edu/cg/middleware.asp](http://www.educause.edu/cg/middleware.asp).
- For more information on the NSF Middleware Initiative, visit <http://nsf-middleware.org>. For questions concerning identity management tools and resources, contact Ann West at [awest@educause.edu](mailto:awest@educause.edu) or [awest@internet2.edu](mailto:awest@internet2.edu).

in place for maintaining security of the covered information. It is no longer sufficient to merely not release private information; we also have an obligation to keep the information secure.

- **Business and ethical stewardship**—Institutions must also consider the requirements of doing business including safeguarding confidential information and intellectual property, and other strategic information. This includes ensuring appropriate access to tenure committee communications, salary and review information, institutional planning, and archive information, to name a few. The institution also has an ethical obligation to protect information that can be, for example, used for identity theft. A very concrete example of this is restricting access to and use of social security numbers in states where no legislation exists to protect them.

### Implementation Issues

While not minimizing the effort involved in implementing the technology pieces, the issues related to policy tend to be the stickiest ones to resolve, requiring the collaboration of numerous campus participants. (See Figure 2.)

#### INTERDEPENDENCY: WE'RE ALL IN THIS TOGETHER

Tying together the access to our applications so their use can be updated, enabled, or disabled quickly is a powerful thing. However, what we do on a daily basis affects many people we're unaware of and small, uncommunicated changes can make for unforeseen consequences.

For example, a new, temporary policy allows returning students to pay their bills a week late. This grace period begins, and the Bursar's Office hasn't received Bob's bill and doesn't update his active status in the SIS system. And as usual, every half hour, the identity management system checks the active status, updates its information, and, in this case, removes the contents of the attributes used in authorizing Bob's access to the library service, health service, course management sys-

tem, e-mail, and departmental accounts. At 7:30 a.m., Bob tries to log on and read e-mail and can't, contrary to the new policy. In this case, the operating policy consequences ripple out to the applications served by the infrastructure and the student is confused.

#### TRADEOFFS: RISK AND SERVICE DELIVERY

A critical part of the identity and access management function is an accompanying security policy that highlights the goals and levels of trust the systems will support. From this (and other things), the technology and procedures are derived. For instance, providing access to a course resource site might require a different security level, than, say, an application that changes a student's financial aid. Looking further, to reset one's password in the first scenario might require answering two predefined questions online and, in the second, visiting a particular office in person.

So what if there's a mismatch between the level of security supported by the infrastructure and that required by the application? Or vice versa? Coupled with increased security is increased cost and decreased risk, but how important is the new application to the institution, and who will pay this increased cost? Is it worth it? And who makes the decisions regarding the tradeoffs? This is where a well developed governance process comes into play.

#### GOVERNANCE: COMMUNICATION IS CRITICAL

Data stewardship policies and ongoing interpretations of them are classic examples of the need for governance. Setting up a definition of stewardship, the responsibilities of the steward as well as the user of the data (application developers) is important for those using the identity management system. The stewardship of the identity management system should be discussed as well. Usually it's a combined management of IT (for the service), data stewards (for the data), and the policy stewards. Additional players including the risk managers and auditors, online service providers and resource managers, application champions, and system users.

A classic example of a problem that the technologists typically receive, but should be considered at policy level is that of a faculty member who wants to give a colleague at another institution access to an online course he is teaching. They are collaborating on research on pedagogy in their field, and he believes that it would be helpful for his colleague to view what's happening in the course. It would require little effort to create an affiliate ID in the identity management system for the colleague and to give her access to the online course and the identities of the students and their grades. However, this raises potential FERPA issues. Would the person processing the request for an affiliate ID know enough to ask the right questions?

Communication and education about the challenges and issues that we each face on a daily basis is crucial. In the most successful implementations, policy examination and interpretation is an integral part of the process and an on-going, rather than a one-time, event. It is critical that all of the groups— data and policy stewards, technology staff, and others—understand both policy and technology issues well enough to identify potential problems as they arise and know how to get them resolved.

## Conclusion

In general, we're all trying to accomplish similar things, such as transitioning to self-managed services for faculty, staff, students, parents, alumni and any constituent the institution wants to maintain a relationship with. In fact, we want contact with more people, earlier in their affiliation with us, wherever they are, and for life. Beyond that, we want these services to work and we want a degree of trust that only those we want to access them do so. Beyond that, we hear rumors of government-sponsored electronic services that are reliant on our campus ability to vouch that a student or faculty member is who they say they are. All this can't be done cost effectively or reliably without an identity management system.

*This material is based in whole or in part on work supported by the National Science Foundation under the NSF Middleware Initiative—NSF 02-028, Grant No. ANI-0123937. Thanks are extended to Mark Bruhn of Indiana University and Michael Gettes of Duke University for their ideas and contributions.*

## ABOUT THE AUTHORS

**Jeff von Munkwitz-Smith, Ph.D.** is the University Registrar at the University of Connecticut.

**Ann West** has a joint appointment with EDUCAUSE and Internet2 to lead the outreach activities of their National Science Foundation Middleware Initiative Award.

*This article originally appeared in the Fall 2004 (Volume 80, No. 2) issue of College & University, and is being reproduced/ distributed with the permission of the American Association of Collegiate Registrars and Admissions Officers. Copyright 2004.*