The Emergence of Identity Service Providers

Ken Klingenstein, University of Colorado, Boulder; Internet2

Nate Klingenstein, Internet2
Overview

Thousands of situations require a person’s identity to be established. Before funds can be withdrawn from a bank, identity is established. Before a book is checked out of the library, identity is established. Before an individual enrolls in college, identity is established.

Of course, the process goes beyond establishing identity. It also involves assessing other criteria, including the person’s role or whether the individual is authorized for certain actions (are there sufficient funds to withdraw from an account? is the individual enrolled in a particular class?). In a transaction-based environment, higher education institutions need to establish the identity and appropriate roles of those with whom they interact, both on- and off-campus.

Although establishing identity is not a new requirement, the implications are different in a digital world. First, there are unique challenges to determining identity in an online environment as opposed to face-to-face. For example, how do you determine who is actually participating in an online chat session? Second, a host of valuable resources (remote instruments such as telescopes or supercomputers, licensed materials such as those held by libraries, or bank accounts) are accessed online based on an individual’s identity and roles. The risks to institutions of allowing unknown or unauthorized individuals access to these resources are immense.

Identification and determination of appropriate roles are required for access management. In a world of network-based resources, there is a range of immediate and pragmatic needs for these types of services. Consider the following situations:

- A faculty member is a participant in a multi-institutional research project. Although located at institution X, the faculty member needs access to supercomputing resources located at institution Y. How does institution Y know that the faculty member should have access to these controlled resources?

- An off-campus student wants access to a licensed database maintained by a publisher. How does the library (or publisher) validate that the student is a legitimate user so that the licensing agreement is not violated?

- A student seeks access to electronic reserve materials from his home. Although enrolled, is the student registered for this particular class?

- A research team from multiple campuses establishes a Web site for private communication and to hold documents related to its project. Researchers at one location manage the site, which is accessed by individuals from other locations. How does the site manager know whether to trust the identity of those logging in to the site? Can this be done in a way that avoids proliferation of user names and passwords for the researchers?

- A campus has an agreement with vendor X that all active faculty and students can receive a discount on the vendor’s products. How does the vendor verify
that an individual wanting to complete a purchase is really an active faculty member or student rather than an alumnus or visiting professional?

The problems reside at both the technical and policy levels. How does one computer determine that the user at another computer is really a member of a specific community? How do applications keep track of identities and roles across multiple communities? In the physical world, such “technical” problems are handled by presenting a library card, an ID card, or a driver’s license.

Whereas most networked access to resources came from on-campus a few years ago, today’s climate is much more nomadic. Individuals use commercial Internet service providers, cable modems, DSL, or Internet cafes to access e-mail, library, and other computing resources. In addition, there has been tremendous growth in the numbers of distance learners, part-time students who access learning environments from work, or those who dial in from home. The transitory nature of higher education “customers” (students graduate, drop out, and transfer) exacerbates their nomadic nature.

In a networked environment, users routinely seek access to a variety of resources controlled by many different organizations, such as publishers, libraries, colleges, research teams, and others. Users are unable (and unwilling) to remember many different IDs and passwords. And individuals commonly engage in transactions with entities other than their own colleges or universities. Organizations are unable to handle the authentication1 and authorization2 of thousands of individuals beyond their own user community. There is a sizable responsibility simply in protecting the security of the ID list, not to mention ensuring that the list is current.

To manage this complex set of relationships and processes, a new category of service provider is emerging—the identity service provider (IdSP). These providers enable people to interact across a broad marketplace of current—and future—services. Current services might include allowing users to have a single sign-on for multiple Web sites. The single sign-on may also allow one to make purchases online, share calendars, or log on to desktop videoconferences. Future uses may let travelers identify themselves to a rental car, at which point the car’s radio buttons automatically set to their personal preferences. Or, imagine the administrative assistant of the provost at one institution being able to seamlessly view the calendars of the provosts in the region to determine the best time to set up a meeting.

Higher education has many needs for identity services. Student identification cards not only provide a photo ID but electronically give access to buildings and resources at many institutions. If a student leaves the institution because of graduation or dismissal or any other reason, access to buildings and services should terminate immediately, whether or not the card is returned. And when researchers share resources on other campuses, they want to be confident that those who access those resources are who they say they and are authorized to use the resources. Note that identity services can include both identification of the individual and the role(s) for which he or she is authorized. Access is often based on role rather than identity. Indeed access by role (or attribute) rather than by identity can preserve privacy where appropriate. A law student, for example, should be able to access restricted library content (Westlaw) and do so
anonymously. However, depending on the contract, an alumnus should not have the same access.

While institutions have always found ways to identify members of the community, an online environment makes identification much more challenging because Web access to courses, information resources, and services combines with e-commerce, from both on- and off-campus. Although users are provided with IDs and passwords, no common infrastructure addresses the needs for identification services on the Internet. For the higher education community, one of the risks of inadequate identity services is the use of campus resources by inappropriate individuals. Greater risks focus on privacy, security, and cost.

Several initiatives under way could provide this middleware identity infrastructure. Each has a slightly different scheme, with none covering all needs. As this market emerges, higher education institutions will need to decide whether they will provide these services themselves or whether they will rely on outside parties. A series of decisions must also be made about who is authorized to use what institutional services, and about how to deal with security and privacy issues.

This Research Bulletin describes the current efforts under way and some implications. The bulletin also highlights specific issues associated with how higher education provides the identity service infrastructure for students, faculty, and off-campus collaborators.

### Highlights of Identity Service Provider Models

Throughout the day, individuals deal with the world from multiple roles or contexts. Most have a work persona and a persona as a private individual, in the context of home or family. There may be other contexts, such as a second job or a role in a community organization or an educational institution.

Five or ten years ago these personae were separated in space and time. In a networked world, however, we may want to move from one persona to another with the click of a key. A worker may log in to an online course during the lunch hour. An individual may study from home rather than on campus.

Within each persona, we want simple and consistent management of identity. The persona should be associated with a single password and a handful of other identifiers (such as e-mail address or passport number). And while an individual’s identifiers are relatively permanent features, other attributes change: A student may later become an employee of an institution, or his permissions to access certain resources may change. Because of this potential for change, it is wise to separate authentication and authorization mechanisms.

Security and privacy are also vital. Security guarantees one’s electronic presence to others and protects that presence against theft or impersonation. Privacy, on the other
hand, protects against the revelation of identity when the user has the right or expectation of anonymity. Privacy also lets users encrypt and protect their intellectual property and personal information. Privacy is often considered a trade-off with security, that you cannot have high levels of both. But experts believe this is only a function of our current tool set and that with the proper design of a middleware system each can be appropriately conserved.

Services for an identity associated with work will likely be provided by the employer. Services for personal identities (for example, as a consumer) will come from other providers. It is unclear how colleges and universities will provide these services. There are a number of solutions currently in development, including Microsoft’s .NET, Magic Carpet, the Liberty Alliance, public key infrastructure (PKI), and Shibboleth.

**Microsoft’s .NET**

The most visible contender in the identity service provider space is Microsoft. The company hopes to move from managing the desktop environment to managing users’ personal information. Not only does Microsoft plan to hold information for intra-realm uses, but it plans to provide this information to sites outside the organization. The Microsoft strategy, consisting of several initiatives, is known collectively as .NET. (And, not coincidentally, Microsoft hopes to move from a revenue stream based today on one-time purchases of software to a monthly subscription service for providing identity.)

In .NET, users’ personal information is stored centrally by Microsoft and used both by Microsoft’s own Web-based services and third-party sites. These third-party vendors, which provide services as diverse as e-mail, calendaring, specialized digital content, or video-on-demand services, contract with Microsoft to access this personal data for their own offerings.

.NET consists of a central security framework known as HailStorm, which uses both standards and proprietary components to provide information about users to satellite sites. This gives users a means to log in one time to access all .NET sites using a technology called Passport. Sites owned and operated by third parties query HailStorm and Passport to find out the elements of a user’s identity. These sites can then use this information to decide whether to grant access to online content, to supply basic information such as name and address, or even to acquire credit card information for billing. HailStorm’s e-commerce services are known as “the wallet.”

Windows XP is designed to interlock with .NET to provide services on the desktop through the .NET infrastructure. If users (on- and off-campus) follow the natural Windows migration path, they will eventually upgrade from Windows 2000 to Windows XP. While users can operate XP without opening a Passport account, it is inconvenient, and there are many XP services, such as network conferencing, that work only with a Passport account.

Note that operating units within Microsoft may compete directly with third-party service providers, for example, by providing calendaring services or an e-mail inbox. This prospect presents risks to competing third parties and to the customer base. For third
parties there is always the risk that Microsoft may implement a feature that puts them at a competitive disadvantage. For users there are privacy concerns. The privacy laws that exist typically protect users against a company providing a user’s personal information to another company; there is far less legislation governing the inappropriate release of information between units of the same company.

**Magic Carpet**

Microsoft’s strategy relies on the desktop providing identity services. Another approach, from America Online (AOL), focuses on the ISP providing those services. Already AOL provides users with identity services for its substantial menu of direct and affiliated content providers. AOL’s development effort, Magic Carpet, extends the scope of its current efforts to something akin to HailStorm. The first released component (Screen Name Service) provides some uniformity of information flow to a user across multiple platforms, such as desktop computers and cell phones. Like Microsoft’s efforts, AOL’s is currently limited to the company’s platform. Neither initiative has the stated goal of interoperability.

**Liberty Alliance**

Interoperability is one of the promises of the Liberty Alliance, a coalition of 38 companies, which seeks to create a federated authentication solution for network identity. In contrast to the proposed .NET infrastructure, the Liberty Alliance believes that personal information should be stored in a competitive and open marketplace of service providers, with individual organizations maintaining this data and sending it to other participants in a secure, trusted way. The Alliance also has a stated goal of maintaining open standards to allow for interoperability with other authentication infrastructures.

The Alliance emphasizes privacy as well. Members of the Liberty Alliance include companies such as American Airlines, American Express, AOL Time Warner, Bank of America, Cingular Wireless, eBay, Fidelity Investments, General Motors, NTT DoCoMo, Sony, and VeriSign. The Liberty Alliance members represent over one billion network identities.

The Liberty Alliance, with a vision of interoperability from any device connected to the Internet, could shape the marketplace. Its goal of federated identity is described as enabling federated commerce:

> In a federated view of the world, a person’s online identity, their personal profile, personalized online configurations, buying habits and history, and shopping preferences are administered by users, yet securely shared with the organizations of their choosing. A federated identity model will enable every business or user to manage their own data, and ensure that the use of critical personal information is managed and distributed by the appropriate parties, rather than a central authority.

Among its challenges will be managing the multiple interests of its partners, with many of them thinking that they should be the primary identity service provider for consumers.
Public Key Infrastructure (PKI)

Unlike the approaches described so far, which intend to use passwords and other mnemonic authentication techniques, a more secure—although more difficult—technology is public key infrastructure (PKI). PKI leverages a powerful asymmetric cryptographic technology based on a user having private and public keys. PKI can go beyond identity services, providing, for example, encryption and signature of electronic documents. If a user signs a document with his or her private key, recipients of the document can verify the originator of the document and the integrity of the transmission.

Unfortunately, PKI faces numerous implementation problems because of technical complexities. For example, vendors have made incompatible assumptions in their implementations of parts of PKI that are not yet codified in standards. The legal trust mechanisms associated with PKI have created very high and costly barriers as well. And PKI, with its orientation towards strong identity, is not well suited for privacy. Although most authorities see PKI as a viable solution, it may take another five years to materialize.

Shibboleth

A new effort from the academic sector—Shibboleth—is built on a model of federated administration. Led by Internet2 and IBM, Shibboleth is designed to support inter-institutional authentication and authorization for access to Web services. A security domain, typically a campus, is free to use whatever authentication scheme it prefers internally; it will then provide identity services information about its users to resources at other sites within the federation. The Shibboleth infrastructure provides a way to transport attributes securely from one security domain to another within a federated system. Shibboleth uses the parts of PKI that work now (PKI among computer systems), while allowing campuses to leverage their existing security approaches. Shibboleth is oriented towards privacy, with users having full control over the release of their attributes.

What It Means to Higher Education

Higher education has historically operated as an open, fluid community. Individuals enter and leave the community frequently (students enroll and graduate), and those with casual affiliations, such as alumni, are often extended privileges such as e-mail. Although campus directories are coming into existence now to store those relationships, managing identities has been a relatively undeveloped process. The need for identity service providers signals a change in this historic approach. The shift is taking place well beyond higher education; the New York Stock Exchange, for example, is also dealing with federated identity issues.4

Higher education must begin actively managing identity and roles. Regardless of the technological approach, colleges and universities will find it a challenge to manage the relationships of their multiple constituencies (students, faculty, staff, alumni, board members, consultants, and so on). Although institutions may maintain directories, the
granularity with which relationships are identified is typically limited. As the marketplace matures, institutions will need to define categories of relationships (for example, professor emeritus or adjunct faculty) and the process by which those roles are assigned. Institutions may ultimately distinguish 50 or more distinct relationships. These identities and roles will need to be rationalized with existing campus systems, such as the personnel system, the student information system, the alumni database, and others.

Once the categories of relationships are determined, institutions will need to decide what privileges are associated with specific categories. In the past, all permissions were bundled with a computer account; identity services will require an unbundling of privileges. Can alumni access digital library materials? Can a professor emeritus have an e-mail account? Can prospective students have customized portals? If contractors need to use the electronic building access system, must they enter the campus directory? What other privileges should they be assigned? Some issues will arise within the institution; others will depend on licensing arrangements with publishers or on state laws. Making decisions about differentiated services will be a challenge for higher education.

Establishing identity and relationships is not enough—the process must be actively managed. Institutions must know when an individual’s roles change. For example, if a student withdraws, his privileges should be automatically cancelled. Identity resolution processes will be required on an ongoing basis as well. How will the institution determine if the Joan Smith who wants to take a continuing education class is the same Joan Smith who works at the university hospital and is entitled to lower tuition?

The cost of providing identity services depends largely on the level of vouching (precision with which the individual is identified). Greater confidence costs more—the individual is initially identified using a government-issued photo ID in a face-to-face setting as opposed to simply signing up online. No one is certain how much users, or higher education institutions, will pay. It is also unclear whether the costs will be separately identified or subsumed in some product. In the banking industry, for instance, the costs of initial identification are part of the existing operation, so the expense of operating a new identity system is marginal. The costs may be absorbed by the relying organization, as with credit cards, or passed along to the user, as .NET anticipates.

Higher education operates both as a business entity and as an academic organization. As a business entity, cost is an issue. Identity services will have a cost, but how much can (or should) higher education pay? If Shibboleth is the system selected, the costs are internal to the institution; if .NET is selected, the expenditure could be significant if a transaction fee is assessed to the campus each time someone accesses a Web site.

Higher education must also view identity services from the perspective of an organization facing unique requirements, including the Family Educational Rights and Privacy Act (FERPA). FERPA limits the release of individual information. How will higher education manage the requirements of FERPA if identity services are outsourced to an organization such as Microsoft? Will vendors be willing to accommodate the unique requirements of higher education?
That identity services are becoming a fact of life for higher education raises concerns over anonymity. Library patrons have historically had the ability to browse the shelves and check out volumes freely and anonymously. Will anonymity be compromised by identity services?

As institutions move toward identity services, several key questions should be asked:

- How do we handle identifying members of our college or university community? Do we distinguish different roles of users? Do we keep these lists up-to-date? How are they linked with the legacy systems that feed or need the information?
- How do we handle providing services? Are all services provided to all users, or are they differentiated based on an individual’s relationship to the institution?
- How will the institution maintain adequate security and privacy, balanced with the need to provide identity services?
- Are we developing an infrastructure that will be compatible with one of the identity service providers?
- What processes do we establish to handle identity resolution needs? What organization on campus manages this process?
- Are identity services something our institution should “in-source,” or is it more appropriate to outsource? If outsourced, is the third party trustworthy?

Identity services are emerging in a number of sectors, including banking, securities trading, and education. Higher education may accept the systems devised by others, such as .NET, or participate in the creation of identity services tailored to its own needs, such as Shibboleth. Now is an opportune time for higher education to begin addressing this new inter-institutional infrastructure that will be required for both the academic enterprise and active participation in a networked economy.

Where to Learn More

- For information on the Liberty Alliance, see <http://www.projectliberty.org/>.
- For information on Microsoft’s .NET, see <http://www.microsoft.com/net/>.
- For information about PKI, see <http://www.educause.edu/netatedu/groups/pki/>.
- For information on Shibboleth, see <http://middleware.internet2.edu/shibboleth/>.

Endnotes

1. Authentication is the process by which the system validates a user.
2. Authorization is the process by which the rights of validated users are determined and those validated users are enabled to use certain resources in accordance with those rights.

3. Not only is Passport proprietary, there are concerns about its security. Several security problems have already been identified, and patched, in Passport. Whether Microsoft will reveal future compromises is uncertain.

4. For example, see

<http://www.simc-inc.org/archive0002/February02/agenda26feb02.htm>.

---

**About the Authors**

*Ken Klingenstein (ken.klingenstein@colorado.edu) is Director, Internet2 Middleware Initiative, and Chief Technologist, University of Colorado at Boulder. Nate Klingenstein (ndk@internet2.edu) is a technical writer for Internet2.*