Federated Identity in Education

Cloud, cloud everywhere, what's a higher ed CIO to do? We didn't always have all these options. Five years ago, just as cloud computing was exploding as a commercially viable, dynamic technology platform, Brad Wheeler, Vice President and Chief Information Officer at Indiana University, posed a question to me while I was serving as CIO at UC Berkeley: “Now that the commercial world is beginning to offer computing services at scale, what must higher education do to leverage services above the campus?” For me, this was a “not if, but when” question and an acknowledgment that distributed above-the-campus computing at national scale was going to be part of our future. Brad and I continued to explore this opportunity, guided by the oft-quoted maxim of Alan Kay, Chief Scientist at Atari and a member of Xerox PARC in the 1970s: “The best way to predict the future is to invent it.” We ultimately engaged with many other campuses in a workshop sponsored by EDUCAUSE, Internet2, and NACUBO to consider the impact of the cloud on higher education. Brad and I published our thoughts in an EDUCAUSE Review article in which we called for an above-campus strategy for higher education.¹

Since that time, technologists and consumers alike have been amazed by the explosion and veritable “alphabet soup” of cloud-based options: IaaS, PaaS, and SaaS (Infrastructure as a Service, Platform as a Service, and Software as a Service) from large and small companies alike. Each option is offered at huge scale, often with per-unit pricing far below what was previously available to smaller organizations running their own environments. Yet though the transformation has been impressive, I believe the real benefit of the cloud emanates not from the improved economics, the flexible capacity, or the global scale but, rather, from the incredible surge of innovation unleashed in the SaaS space, enabling design for scale while requiring only small pieces of cloud infrastructure during the development phase. No longer does a company (or a campus) need huge capital investments in data centers, servers, or storage to develop a new solution. So, a campus simply needs to find the service, sign a contract (or use a credit card), and start using the service, right? Not so fast... Having all those SaaS options, ranging from large enterprise systems to the plethora of small niche solutions, may be great from an innovation and opportunity perspective, but the wide variety of options and choices presents a challenge that didn't exist when the systems were inside a data center. Specifically, while working to quickly and easily take advantage of those services, how does a campus maintain a common operating environment of shared applications and shared data without having to impose draconian central control before a department or an individual can use make of those services? How does a campus streamline the needed integration work? The answer should start with something that every institution has already (hopefully) been moving toward: a comprehensive federated identity strategy. The approach should meet campus needs not only today but also into the future—specifically a future in which higher education institutions work together and depend on each other as never before in order to achieve the necessary scale in educational delivery.

A Solution Ten Years in the Making

For over a decade, Internet2 member institutions have been supporting many aspects of establishing the underpinnings of federated identity. Yale created CAS (Central Authentication Service), MIT developed Kerberos, Internet2 developed Shibboleth, Grouper, and more. These technologies have been adopted by hundreds of institutions nationally and globally. In fact, many campuses and labs (over 480) are already participating in InCommon (http://incommon.org), the national higher education federation that allows anyone physically located on a participating institution to use his/her credentials assigned by the local campus for services both on and off campus.

Launched by a host of campuses in 1994, InCommon aimed to make services developed by one campus available to an individual at another. To establish these services, it built the underlying middleware (which focused on open cross-platform environments rather than those dependent on a single provider) as open source for broad adoption. Now these technologies are deployed extensively across higher education in limitless use cases. Moreover, the emergence of commercial cloud offerings has expanded the list of services where those credentials can be used. When deployed at the campus operating as an Identity Provider (IDP) and subsequently matched with a correctly configured Service Provider (SP), the use of fully qualified InCommon federated credentials offers the following benefits:

- **Speed of Deployment.** By using existing campus credentials, an institution can make a service available quickly, at both the enterprise and the individual levels, with no need for additional issuance of individual application credentials.
- **Policy Control.** Federated InCommon Credentials are issued by the institution, and only that institution, following its own policies. There is no need to worry about having to evaluate the policies of the application provider.
- **Increased Security.** Authentication breaches often lead to critical data loss. Since the service provider doesn't have access to the institutional credentials, a breach of the provider's environment will not result in the compromise of campus credentials.
- **Ease of Use.** There are no more forgotten individual passwords across countless applications. Instead, community members use their campus credentials to log in to each service that has been activated as a campus service offering or solution.
- **Data Protection.** A key to preserving institutional data is, first,
knowing where institutional data resides. An institution can support the adoption of institutionally acceptable services by encouraging their use through federated credentials.

- **Provisioning and Deprovisioning.** By using campus credentials matched with the release of attributes (i.e., additional information indicating faculty, staff, or student status), institutions can provide access to one constituency's group of services while minimizing or removing access for another.

So, to take advantage of all these benefits, an institution simply needs to join InCommon, right? Not exactly . . . A campus first needs to make sure that it has implemented a local IdP, which must be configured to be properly integrated into its local identity system that maintains accurate information about campus constituents. Fortunately, the needed software and middleware standards are all open source. Historically, those components have included the following:

- **CAS (Central Authentication Service).** Originally developed at Yale, CAS is now part of the Apereo Foundation (https://www.apereo.org/cas). The original open-source single-sign-on component, CAS is generally used in cases where the service it supports is not going to be exposed outside of the campus boundaries through federation.

- **Shibboleth Federation Software.** A standards-based, open-source software package for web single sign-on across (in the form of a federated service) or within organizational boundaries. Shibboleth provides extensive support for informed authorization decisions for services in a privacy-preserving manner.

- **Grouper Toolkit.** An open-source enterprise access-management system for highly distributed environments, Grouper enables an institution to operate a central access-management system that supports both central and distributed administration.

Although these packages have been downloaded thousands of times around the world, comprehensive installation has not been an easy task. Community members have worked together to improve technical skill, training, and expertise in these solutions, but to date, many institutions have completed partial implementations and/or have relied on widely deployed commercial products (e.g., Microsoft Active Directory and Oracle Identity Manager).

**Big Tent: Trust and Identity for Higher Ed**

What if an institution has limited technical resources? This is where the Trust and Identity in Education and Research (TIER) project comes in. TIER (http://www.internet2.edu/products-services/trust-identity-middleware/) is a multicampus partnership to create an on-premises, fully integrated version of these (and several new) middleware components as an “identity management in a box” solution for higher education institutions to install locally. Additionally, new components will be architected to extend campus services into the cloud, providing unprecedented benefits of scale in areas such as person registries, tools for applicants, and integration portals for commercial services.

TIER is intended to be an essential asset and infrastructure for higher education while addressing the needs of campuses at various stages of maturity in Identity and Access Management (IAM) solutions. Those stages are a spectrum that can roughly be categorized as Emerging, Established, and Advanced. The fundamental objectives of TIER are to provide a common framework for campus IAM components whose adoption enables campuses to increase their IAM maturity; and to support the means by which larger, national-scale benefits can be achieved, including

1. a consistent IAM approach that advances interinstitutional research;
2. a shift to managing attributes rather than identities, in recognition that future students will have multiple well-established digital identities that they want to maintain; and
3. a way to provide fully supported, distributed IT services in terms of both delivery method (on-premises and in the cloud) and location independence (campus-based and global users).

The TIER project will provide a coordinated effort to build on and extend current investments, enhance the technologies to simplify their deployment, and package the solution to achieve the goals of broader adoption and increasing IAM maturity. Whenever possible, the effort will follow the principle of integrating the existing best-of-breed solutions into a more comprehensive set of component solutions that will satisfy a range of needs—from institutions with limited technical resources to those with significant complexity. That plan includes integrating with commercial components that the community feels are a critical part of the collective future strategy as well as extending the open-source pieces of the past. As milestones are delivered over multiple phases during the next three years, the community goal is to have a properly integrated set of components that are designed to be deployed on-premises (at a campus site) in concert with enriched services delivered from a community cloud. This approach will enable all participating campuses to be better prepared to provide and access services both on and off campus.

Getting federated identity “right” is critical to maintaining the privacy of community participants and also their ability to create, educate, and collaborate. To get this right, we all need to work together to invent the future for our community, furthering the kind of cross-institutional open exchange that makes higher education such a strong force for innovation and advancement.

**Notes**

2. Even though TIER is just launching, don’t wait to start on your path to federated identity. Many resources are available online at http://incommon.org. You can also join us by e-mailing info@internet2.edu.

Shel Waggener (swaggener@Internet2.edu) is Senior Vice President at Internet2.

© 2015 Shel Waggener