

Collaborative Tools Strategy

University of California, Berkeley

Spotlight: Identity Management

In the Campus Collaborative Tools Strategy for UC Berkeley, Goal 4 is to "Provide enhanced identity management services." This Spotlight document provides more in-depth discussion regarding that target.

At the core of most types of online collaboration is a layer of identity management services, making it possible for campus communities to control who collaborates together online, and – in conjunction with access control services – what privileges they will be given within various collaborative contexts.

These services make it possible to formally recognize the identities of people collaborating online, to verify with reasonable confidence that they are who they claim to be, and to specify their privileges within those contexts, whether based on role or group memberships or otherwise. When well designed and implemented, these foundational-level services can help make it easy and natural for partners to collaborate within and between units, and across multiple organizations.

IST and its campus partners have been moving towards the adoption of an enterprise-wide identity management architecture. Recent steps include the adoption of the Central Authentication System (CAS), which is used widely across higher education; and licensing of Sun Identity Manager, an enterprise level system which can potentially help automate much of the process of creating, updating, and deleting user accounts across multiple IT systems. Concurrent changes in governance structure are also taking place to improve the campus's abilities in this area.

In addition, the campus is participating in higher education- and UC-wide identity federations, to adopt common standards around data, technologies and practices, and to build networks of trust between participants. This work may ultimately make it easier for members of the campus community to use applications hosted by other higher education partners, as well as to allow members of other institutions to use campus applications.

For a summary of current and planned activities of IST's CalNet team in this area, please see:

- Dedra Chamberlin, "UC Berkeley identity management (IdM) business needs and technology approaches," *Berkeley Computing and Communications*, Spring 2008 (<http://istpub.berkeley.edu:4201/bcc/Spring2008/1147.html>); and
- Dedra Chamberlin, "Federated Identity Management," *UC Berkeley iNews*, September 18, 2008 (<http://inews.berkeley.edu/articles/Fall2008/idm-fim>).

There are several areas in which this campus identity management infrastructure can be enhanced to better support online collaboration. Some of these areas are already reflected in campus work and planning, while others represent future directions.

1. **Make it easier for non-campus affiliates to participate in online collaboration with UC Berkeley people**

A growing number of collaborative activities conducted at UC Berkeley involve participants from other higher education institutions, governmental bodies, non-profit groups, and industry. Adding these

participants to online collaborative contexts at UC Berkeley is often handled in either of two general ways, depending on the collaboration tool in use:

- Requiring that participants must first be added as campus affiliates to the Human Resources Management System (HRMS), by a person authorized to do so.

Once added within HRMS, certain types of affiliates are then automatically added to the CalNet Directory Service within 24 hours, and can begin to use collaborative tools that require a CalNet identity.

- Facilitating the creation of *ad hoc* user accounts simply by entering participants' email addresses, or similar expediciencies.

This is how one can grant accounts in bSpace to non-campus collaborators. This method is also used by a number of collaborative tools in the Internet "cloud."

Neither of these approaches is fully satisfactory:

- The first approach, adding outside people as affiliates in HRMS, is frequently regarded as cumbersome, although there may be some ways to help streamline that process.
- The second approach, using email addresses as a proxy for identity, has the virtue of convenience. However, it has significant shortcomings related to security and management control, rendering it inadequate outside of casual collaborative contexts.

In response to this problem, in November 2008, the CalNet team launched a Guest Account Task Force. This Task Force is looking at campus-wide needs for guest accounts and options for creating them; its work encompasses:

- Establishing a definition for guest accounts.
- Proposing a service eligibility model for guests.
- Developing a technical solution for provisioning guest accounts into our campus directory so that departments can leverage our single sign on infrastructure for guest access.

Ultimately, a comprehensive solution to this problem may, in part, require that the campus identity and authorization infrastructure interoperate with emerging federated identity management specifications, not only those used within the higher education community but also with those from the industry and consumer spaces. These standards-based approaches offer the potential to make it more straightforward to add outside people to campus collaborative contexts, and also – as an additional benefit – to make it easier for members of the campus community to participate in collaborative contexts hosted by other higher education institutions and outside providers.

The CalNet team is actively participating in two identity federations, InCommon (<http://www.incommonfederation.org/>), whose participants include many prominent higher education institutions, as well as government bodies and corporate partners; and UCTrust (<http://www.ucop.edu/irc/itlc/uctrust/>), whose members include University of California campuses and the UC Office of the President.

Both InCommon and UCTrust aim to build a framework that would allow members of any participant to authenticate to, and provide selected identity attributes (such as affiliation status) to, the online systems of any other participating institution. While both federations are based on a common technical platform, Shibboleth, UCTrust extends the work of InCommon to facilitate cross-institutional access, exclusively within the University of California system, to more highly sensitive online services. As of January 2009,

the campus has been a member of those federations for one year, and the CalNet team is running a Shibboleth Identity Provider.

To further extend the scope of these efforts to additional partners in education, industry, government, community groups and the public, there may also be merit in the campus's monitoring or participating in the activities of Project Concordia (<http://projectconcordia.org/>) and/or the Identity Commons Community (<http://idcommons.net/projects>). These are complementary community initiatives that are both working toward interoperability of technologies related to online identity management.

The technologies on which they have focused include, in part, various approaches to managing trust around asserted identities, such as the relatively lightweight OpenID, and two identity suites each based on competing technologies: SAML (core to Shibboleth, which in turn is at the heart of InCommon and UCTrust, and now also used by Liberty ID-WSF); and WS-Trust (used by Microsoft's CardSpace and WS-Federation).

2. **Provide directory services that can assist with managing memberships of campus communities, especially communities of practice.**

As noted in Section IV: Findings, a great deal of campus collaborative work occurs within the context of informal campus communities. These communities of practice consist of people who learn together and share common goals in both academic and administrative contexts. One example is the community of campus employees who must work together to effectively serve graduate students, not only within the Graduate Division but across many other academic departments and administrative units. Another is the community of campus affiliates working toward the commercialization of biofuels, spanning areas as diverse as basic research in chemistry and biosciences, ecology and finance.

Unlike formal affiliations that are discoverable via campus data, the membership of these communities often crosses formal boundaries, such as campus unit, job title, academic discipline and student major. It is often difficult for new members of the campus community, or those who have recently taken on new roles, to find and become affiliated with their relevant communities of practice, as well as for existing members to track changes over time to their community's membership.

There is value in exploring whether the CalNet infrastructure can be extended to better serve communities of practice. One could readily envision, for instance, that community of practice affiliation in CalNet might provide authoritative source data that could be used to populate dynamic mailing lists for these communities, to automatically provision accounts and access privileges in collaborative workspaces associated with these communities, and the like.

Another application might be to help connect new faculty, students and staff to communities of practice relevant to their fields, intended majors, or areas of expertise. This might take place at any point but might be particularly useful prior to their arrival on campus. For instance, ETS's Mara Hancock has expressed interest in connecting newly admitted students to community worksites in bSpace relevant to their majors or interests.

The CalNet team's first priority, with respect to roles and group membership, is to establish core, institution-wide roles that confer access to core business applications. The CalNet team then hopes to build on this work, by exploring options for using Sun Identity Manager to allow the *ad hoc* creation of roles, which could be defined to include membership in communities of practice, and the associated access privileges conferred by such membership. While the team acknowledges "a lot of work to do in this area," they are working closely with campus stakeholders to learn more about what these "communities of practice" look like, how delegated authority to create them might work, and how access rights should be granted.

By providing direct support for communities of practice, the campus's identity management infrastructure would allow members of the campus community to work together in ways that they want to — but can't — today.

3. **Make it possible to create consolidated profiles for the campus's vast and growing pool of alumni and past affiliates.**

... while the UC Berkeley endowment also saw healthy growth [... in 2007 to a] total of \$837 million - it is dwarfed by Stanford's [\$17.1 billion endowment,] even though Cal educates more than twice as many students. Another way to look at it: Stanford has \$1.1 million per student socked away in its endowment, while UC Berkeley holds just \$23,900 per student.

—Carrie Sturrock, "Stanford endowment soars, Congress takes notice,"

San Francisco Chronicle, January 24, 2008

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/01/24/MNCLUJSHN.DTL>

Each person who passes through the campus's classrooms, offices, and labs often builds a portfolio of multiple past or current relationships with the campus over time, as well as with campus people. Providing access to profiles that more fully capture the totality of each person's campus affiliations – past as well as present – and their relationships with campus people, offers the potential to help the campus better draw upon one of its greatest untapped resources: its alumni and past employees. This, in turn, may help over time help bring about deeper, and more meaningful and personally satisfying, contributions to the campus, both participatory and financial, from the campus's extended community.

To put this another way: to better engage our hundreds of thousands of alumni as collaborative partners, in current and future campus initiatives, we need to start getting to know them better.

Frequently, Berkeley's people have had multiple relationships with the campus. As Zane Cooper of the Haas Business School has observed, a particular person may, at various points in time, be a student in the School's MBA program, a member of an Institute at the School, and an industry contact through whom students might be placed into internships or jobs. That person might arrange to bring Haas faculty into their industry setting, as instructors or consultants. They may come back to teach a class, give an individual lecture, or take additional coursework, either within the Haas School or elsewhere on campus. Finally, they may also donate, financially or through volunteer work, to the School or to campus programs of particular interest to them.

Making the totality of each person's campus affiliations – as well as their associations and contacts with campus people, if that is also feasible – available in the form of consolidated profile data might help the campus take advantage of many additional – and perhaps more finely targeted – opportunities to invite past affiliates to remain closely connected to the ongoing activities of the campus and its units and communities.

Reaching this goal may be challenging. Campus directory services typically don't store this breadth of data, nor do they often preserve much historical data for ongoing use. Customer relationship management (CRM) systems - a type of collaborative tool mentioned elsewhere within these recommendations - may do so. However, individual CRM systems and comparable systems that track contacts and relationships are often used for specialized, constrained purposes, such as in managing fund raising from alumni, in coordinating services provided to customers by several related service units, or in managing a single campus unit's relationship with its community. As a result, they may not typically be integrated with the campus identity management infrastructure or with other institutional data sources.

Nonetheless, finding ways to aggregate historical and current data about the many affiliations (and possibly also personal associations) of the campus's alumni and past employees - as a centralized service layer, whether part of the CalNet infrastructure or otherwise – may present opportunities of sufficient value that there may be merit in further exploration of this area.

As one possible starting point, in 2008, the CalNet system added over 400,000 alumni to the CalNet Directory Service, and perhaps this may serve as a foundation for the future addition of data related to these affiliates' relationships with the campus. There are also future plans to add other types of "advancement constituents" - parents, donors and other University Relations-identified affiliates - to the Directory.

Another promising area of investigation might be to look at integration opportunities with the numerous other online profiles that campus people use to declare their affiliations, interests and skills: with the California Alumni Association; social networks like Facebook and LinkedIn; academic publishers; and other institutions, both within and outside of the higher education community.

4. **Begin laying the groundwork for future expansion of the CalNet infrastructure to add authorization services**

Currently, the campus' CalNet infrastructure provides centralized directory and authentication services which are used by the vast majority of campus online applications, collaborative and otherwise:

- Directory services, which provide authoritative directories of data for campus people, organizational units, and other key elements of the campus online environment.
- Authentication services, which help identify whether a person, a computer program, or a similar actor is highly likely to be who they claim to be, a key prerequisite to granting them access to campus online systems and services.

There is an obvious candidate to be added as a third component of the CalNet infrastructure: authorization services, which identify the role(s) in which a campus person (or some automated stand-in for a person) may carry out their work, and the context in which they can perform that role. An example is "'Person (or equivalent) X' is granted the role of 'approving purchases' within the context of 'Department Y'." Any person assigned that role, within that context, is automatically granted the privilege to approve purchases for Department Y. That privilege can be automatically revoked, or otherwise automatically changed based on business rules, when the person leaves that role.

The potential benefits that a centralized authorization service might provide to collaboration tools include:

- Automatically providing new members with access to the tools used by their collaborating communities.

An authorization service may make it possible to automatically create, change, and revoke accounts and their privileges in multiple collaborative tools, based entirely on changes made in a single, central place to a source of authoritative campus data. For instance, a project lead role may be created for a specific project. This would allow any person in that role to automatically receive the privilege of assigning other members to the project. In turn, this would automatically give those members, as soon as they are added to the project team, appropriate access to a project workspace, mailing list, file share, standalone wiki, web conferencing tool,

and any other collaborative tools used by the project team. In contrast, a team or project lead today must create and manage each member's account individually, within each of these separate tools.

- Enhancing the functionality of specific collaborative tools.

As one instance, collaborative tools for designing, building and deploying simple online workflows could potentially greatly benefit from a centralized authorization service at UC Berkeley. Having the ability to centrally define a small set of common campus and unit-level roles that would could be reused throughout many of the workflows created by programmers, managers and business analysts at both campus and unit levels, and building an infrastructure to initially manage just those roles, would significantly leverage the utility of those workflows.

- Providing a mechanism for helping to identify collaborative activities, including communities of practice and other ad hoc or informal collaborating communities.

By creating roles related to non-formal collaborative activities, this may inherently create a *de facto* repository that can be used to identify the existence of such activities, as well as to help campus and community people locate their work products, and to provide contacts for inquiring further about them. Similarly, data about roles and privileges could also be used to help members of a community automatically locate the set of collaborative tools to which they have been granted access.

Offering an authorization service is a relatively long-term goal. To date, few higher education institutions have formally explored, much less implemented, centralized authorization services, and only a few – MIT and Cornell among these – have long-term experience with them.

The ability to implement role-based access control - an ability that lies at the core of any authorization service - is one of the primary drivers of the CalNet team's Sun Identity Manager project. In 2009, the team will be helping launch a new subgroup of the Identity and Access Management Steering Committee, called the Identity, Access and Affiliation Workgroup. The charge for this group is to develop an approach for establishing roles on campus, both institution-wide roles and a mechanism for allowing departments to create roles to manage access to departmental applications.

To make this a reality, extensive groundwork will be required, as will active, ongoing participation from many parties across the campus. These include the campus departments and systems which provide authoritative identity data to the identity management system (such as HRMS, Student Systems and UREL), and system managers across the campus. Roles and privileges will need to be defined; business processes will need to be set up for associating each member of the campus community with their set of roles, and keeping this data up to date, over time; and individual campus and departmental applications, collaborative and otherwise, will need to be integrated with this new, centralized authorization service.

The enormity of this latter integration task shouldn't be overlooked: it will be considerably more involved than the relatively straightforward task of integrating a web-based collaboration tool into CalNet's authentication service, CAS. At some of the nation's higher education institutions that have led the way in implementing roles-based authorization, just a few core campus business applications, such as large financial or human resources systems, have so far been integrated into their authorization infrastructures.

The campus's involvement in the consortium of higher education institutions working on the Quali Student project may offer some noteworthy opportunities for integration, however. That project is designing a set of foundational services that may be capable of being integrated with a centralized authorization service, upon which a variety of campus applications - initially within the student services arena - can be built. To the extent that the campus's future student systems may be based on Quali Student-developed services, they may be relatively amenable for integration with a roles-based authorization infrastructure.