User Provisioning Use Cases

User Provisioning Use Cases

This document describes use cases within the University of California that were considered by the design team. While most have already implemented *ad hoc* provisioning solutions, they are characteristic of applications we expect to see in the future.

Use Case	UC-Wide?	Outsourced?	Responsible UC Location	User Community	Provisioning Already Deployed?
Connexxus	Y	Y	UCOP	UC travelers	Y
The Human Resources Learning Management System (HRLMS)	Y	Y	UCOP	UC employees, plus others	Y
UCLA Administrative Applications Shared by UCOP and UC Merced	N	N	UCLA	Most employees	Y, but considering a replacement
Service-now.com	N	Y	UCLA	Most employees	Y, but needs improvement
Ethics Point	Y	Y	UCOP	A few delegated employees per campus	Y
e-academy	Y ?	Y	Participating campuses?	Significant number of employees	N

Connexxus

Connexxus is a travel booking system that incorporates UC's rates negotiated with airlines, hotels, etc.; Single sign-on is implemented via UCTrust /Shibboleth, but travelers must be known to the system before a login is permitted, so all campuses produce a nightly feed that is sent to Trondent, the company that was contracted to perform the user management and authentication for Connexxus. This process is described in System Design Issues for Connexxus. [At Trondent's request, access has been restricted to that document. Only participating ITLC groups have been allowed access.]

Some relevant aspects of this use case:

- Anyone affiliated with a campus may, potentially, be a traveler, not just employees or students.
- Not all campuses send the same information about their travelers, although all campuses share a common file format for their feeds.
- The fact that travelers are sent to the system on a nightly basis prevents creating new travelers on demand.
- The unique key for all feeds is eduPersonPrincipleName, which provides the "join" with Shibboleth assertions at the start of online sessions with Connexxus.

The Human Resources Learning Management System (HRLMS)

The HRLMS system's initial application was compliance-related training for UC employees. At some campuses, it has also been used for other forms of training, not necessarily for employees. Users must be created in the HRLMS before their first login. Basic information about employees is extracted from UCOP's copy of the campus employee records. Campuses can add additional learners and enhance the information provided about employees by creating a nightly feed to a system at UCOP that merges all of the sources of user information and sends all users to SumTotal, the company that has been contracted to operate the HRLMS. This is described in User Provisioning and Authentication for the SumTotal Learning Management System at the University of California.

Some relevant aspects of this use case:

- Anyone affiliated with a campus may, potentially, be a learner, not just employees or students.
- All campuses send the same information to the merge program at UCOP, in the same file format.
- The fact that learners are sent to the system on a nightly basis prevents creating new learners on demand.
- There are two options for the "join" with Shibboleth assertions, UCnetID and UCTrustCampusIDShort, because UCnetIDs are currently assigned reliably only for employees. UCnetIDs are used for employees, and UCTrustCampusIDShort is used for others. There is, however, a current project to assign UCnetIDs to learners who are not employees at certain campuses.

UCLA Administrative Applications Shared by UCOP and UC Merced

UCLA operates several key administrative systems, including Financial, Purchasing, and Payroll for UCOP and UC Merced. These systems rely on DACSS , UCLA's access management system, to manage user access. There are currently approximately 7500 users across 3 campuses using these applications. UCLA is currently in negotiation with another campus to provide administrative systems hosting.

These applications draw user data from the Payroll system and email data feeds. UCLA receives daily FTP feeds from UCOP and UC Merced to populate email address data.

Issue # 1: Federated Access Management Dilemma

At their core, these major administrative systems are all mainframe applications. However, many have connected web application components. In 2009, UCLA migrated all of the involved web applications onto Shibboleth. The intent is to federate them in 2010.

Security administrators from all 3 campuses sign in to DACSS to manage user access in these applications.

Right now, all access rules are tied to UCLA's mainframe ACF2 credentials. UCLA maps its UCLA Logon ID (used in Shibboleth) to a user's ACF2 credential and presents that information via Shibboleth attribute response during sign in. As the applications federate, at least 3 IDP, many SP, and a single Access Management System will need to work together.

- PROBLEM: the UCOP and UC Merced IDPs know nothing about DACSS.

Issue #2: Data Provisioning Problems

UCLA currently receives separate email feed from UCOP and UCMerced to populate DACSS and PAN for transaction and audit notifications. The current daily FTP feed could use improvement. The merge and change detection routine is complex and error prone.

Ideally, the email data should should come through each campus's IAM system.

Service-now.com

Service-now.com is a popular ITIL compliant ITSM application. It is a cloud-based, hosted solution. UCLA has adopted it for its ITSM implementation. UCSF and several other universities have also adopted Service-Now as well.

At least at UCLA, the intent is to eventually allow all IT service consumers (which pretty much means everyone at UCLA) to sign in to submit and track submitted incident tickets and service requests. Similar to LMS and Connexxus, Service-now.com receives a daily feed of employee data from UCLA. In Service-now.com's case, UCLA presents a LDAP interface. Service-now.com refreshes the data daily from it.

Relevant Points:

- Service-now.com supports SAML 1.1 for federated sign-on. UCLA has integrated it with its Shibboleth implementation.
- Service-now.com relies on the feed not only to populate user accounts, but also to create a search directory for Service Desk workers to look up caller information.
- The current user identifier used for record matching is eduPersonPrincipleName.
- The daily refresh is far from ideal. Not only does it prevent on-demand user provisioning and de-provisioning, the merge/change detection routine is complex and error prone. It also does not scale well as the user count grows.

UCLA's current deployment is bilateral (i.e., all users have to sign in using UCLA's IDP). However, because UCLA provides administrative application hosting services for other campuses, users from other UC's will eventually need to sign in to Service-now.com. We'd like to push Service-now.com to integrate with other UC IDPs. But that means other involved IDPs will also need to provide comparable user data feeds to service-now.com.

Ethics Point

Ethics Point was deployed by UCOP in 2009 to support UC's management of "whistle blower" incidents. It has approximately 100 authorized users spread over UC's locations who manage the incidents; it also supports anonymous access for reporting incidents. Each UC location has an officially-delegated person who authorizes access for others at that campus. Since Ethics Point is already deployed, it will not participate in our project, but the use case is interesting.

e-academy

e-academy is an electronic software distributor. It has partnered with Microsoft to deliver software download service to UC employees who are eligible to purchase MS software under UC's Microsoft's Work at Home program.

e-academy is a member of InCommon, and has integrated its web site with several other InCommon institutions. UC Trust and UC Technology Acquisition Support group are working with e-academy to enable qualifying UC employees to sign in to e-academy through Shibboleth to download Microsoft software.

Because UC's unique licensing terms with Microsoft, e-academy and Microsoft requires the campuses to assert an individual's eligibility to participate in the program before download occurs. There are generally two options to satisfy this requirement:

1. Assert an individual's eligibility to download at Shibboleth sign-in time. One possible attribute to use is eduPersonEntitlement.
2. Periodically provide e-academy with a list of eligible individuals. At sign in time, e-academy would check the identity of the signed-in individual against this list to determine eligibility.

e-academy only checks an individual's eligibility during sign-in time. Because there is no requirement for out of band data update, option 1 is likely preferable.