Selected Use Cases

- **Course Deadline Extended** -- A student in Dr. Schonfeld's Ordinary Differential Equations course is unable to attend the final exam due to an authorized absence (a death in her family). Professor Schonfeld has removed access in the LMS to her class notes for the prior semester's students, since the semester is at an end, but she makes an exception for the student at the request of the Dean, and grants her access to the course space in the LMS for an additional week in order to complete studying for the make-up exam. One week later, the student's access is automatically removed by the system.

Proposed Solutions: Grouper, perMIT, Rice, Spocp

A policy service perspective on Course Deadline Extended

- **Old and New Payroll Clerks** -- Gina, an administrative assistant in the Department of Chemistry, vacates her position in the department to take a new position in the Office of the Comptroller. Gina has been the department's payroll clerk for a number of years. The department chair chooses his executive assistant, Marcus, to take over as payroll clerk for the department. As payroll clerk, Marcus will need access to sensitive payroll information about non-exempt employees in the department, but will not need access to faculty salary information or student records. The department chair logs into an access management system and designates Marcus as the new payroll clerk for the Department of Chemistry. In so doing, he grants Marcus a collection of rights within various financial applications appropriate for a departmental payroll clerk in his department, and Gina (who is still employed by the university and still recognized by the authorization system as a user) has her payroll clerk privileges for the Chemistry department revoked. *(Single authority identified organizational hierarchy grants multiple related privileges collected by role on multiple target resources to single subject **and** revokes mulitple related privileges collected by role on multiple target resources from single subject)*

Proposed Solutions: Grouper, perMIT, Rice, Spocp

A policy service perspective on Old and New Payroll Clerks

- **Dorm Access for Residential Advisers** -- For reasons of safety and security, access to student housing on the main campus of the university is tightly controlled. Dormitory doors are magnetically locked and protected with ID card readers wired to the university's "UniCard" system. Between 8am and 10pm daily, all student ID cards will open all exterior dormitory doors, but between 10pm and 8am, access is restricted to those students living in each dorm. Residential Advisers (RAs) constitute a special case, in that they require 24x7 access to multiple dorms within the residential quad in which they reside. When John encounters a family crisis and decides to take a mid-semester leave of absence, Residential Life arranges to make Richard the RA for the North Campus quad. Res Life staff identify Richard as an RA in their housing system, and based on information in the housing system regarding the location of his room on campus, a privileging system grants Richard 24x7 access not only to his own dormitory but also to the five other dormitories in his quad. When the Registrar places John on leave of absence in the registration system, the privileging system recognizes that his special access is no longer valid, and revokes his RA privileges

Proposed Solutions: Grouper, perMIT, Rice

A policy service perspective on Dorm Access for Residential Advisers

---

- **Professional Organizations and Federations** -- A librarian at the college's main library agrees to proctor a survey on behalf of the American Library Association (ALA) of higher ed librarians. The survey seeks to gather information about successful and unsuccessful strategies for managing electronic periodical subscriptions. The survey is intended to target a specific audience - librarians within higher ed who are themselves members of the ALA. Membership in the ALA can only be authoritatively asserted by the ALA itself, while affiliation with colleges and universities can only be authoritatively asserted by those colleges and universities. Fortunately, the ALA is party to an identity federation in which hundreds of higher ed institutions participate. The ALA sets up a web-based survey application using federated SSO services that allows librarians working at institutions within the federation to authenticate through their "home" organizations and gain access to the web application. The web application subsequently determines whether to grant them access to the survey itself based on the status of their membership in the ALA (as determined by direct inspection of the ALA's membership roster).

Proposed Solutions: Grouper, perMIT, Rice
A policy service perspective on Professional Organizations and Federations

---

- **Drug Restocking Approval** -- Nurse Wilson notices during a routine inventory review that the Oncology ward's drug cabinet is running low on a particular anti-emetic drug. The anti-emetic is a scheduled substance, so her request to the Pharmacy for restocking requires approval by both her supervisor and an attending physician in Oncology. The Pharmacy system detects the approval requirement and routes the request to the head Oncology nurse, then to the on-call Oncologist for approval before filling the order.

Proposed Solutions: Grouper, perMIT, Rice

A policy service perspective on Drug Restocking Approval

- **Delegated Directory Administration** -- Bill is one of three IT administrators in the Department of Chemistry within the College of Arts and Sciences. As part of his departmental duties, he manages both Windows-based desktops on faculty and graduate student desks and a cluster of Windows-based fileservers. His systems are all joined to an enterprise Active Directory domain which also incorporates user objects for all the university affiliates in the enterprise identity management system. Due to disk space exhaustion, Bill needs to relocate the home directories of roughly half of his faculty from their current fileserver to a new fileserver. He migrates the relevant data, and then needs to update attribute information in the enterprise AD regarding the path to his faculty members' home directories. His status as an IT admin in the department confers on him the ability to update the homeDirectory and homeDrive attributes for users in his departmental OU within the central AD, and he successfully updates his faculty members' information using standard Microsoft tools. Later, when Bill mistakenly attempts to update one of his faculty member's msExchgHomeServerName values, he is prevented from saving the change, since his rights as an IT administrator in the department do not extend to overriding the campus IDM systems' selection of an Exchange home server for his users. Still later, while Bill is vacationing in the Swiss Alps, his departmental fileserver is destroyed in a machine room mishap, and the faculty whose home directories were moved must be restored from tape to yet another server. In Bill's absence, Patrick, who works for the College's IT administration, is able to use

his college-wide privileges as an IT admin to update the same homeDirectory and homeDrive attributes for Bill's faculty. When, upon his return from Switzerland, Bill takes a position as a departmental support manager in another department, his privileges regarding Chemistry faculty attributes are automatically revoked.

Proposed Solutions: Grouper, perMIT, Rice

A policy service perspective on Delegated Directory Administration

---