Use Case Tabulation

Paccman Use Case Classification

- Business Operations Use Cases
  B-1, B-2, B-3, B-4, B-5, B-6, B-7, B-8, B-9, B-10, B-11, B-12, B-13, B-14, B-15,

- Academic Use Cases
  A-1, A-2, A-3, A-4, A-5, A-6, A-7, A-8, A-9, A-10, A-11, A-12, A-13, A-14, A-15, A-16, A-17, A-18, A-19, A-20, A-21

- Residential Life Use Cases
  RL-1, RL-2

- Library Use Cases
  L-1, L-2, L-3

- Medical Use Cases
  M-1, M-2, M-3, M-4

- Guest Use Cases
  G-1, G-2

- Federation and VO Use Cases
  V-1, V-2

Gartner Classification of Authorization Use Cases addressed by XACML

- Relational
  - B-1,B-2,B-6,B-10,B-11,B-12,B-15,A-1,A-2,A-3,A-4,A-6,A-7,A-10,A-11,A-13
- Contextual
  - B-3,B-4,B-13,B-14,A-8
- Dynamic
  - B-7,B-8,A-5,A-9
- Federated
  - B-9,A-12
- Fine Grained
  - B-5

Background

The privilege and access management problem space is large, spanning virtually every facet of our organizations. As we consider avenues to solving problems in the space, the shear breadth of the space can become quite daunting. During Educause&Internet2 CAMP in 2009, we began the process of collecting use cases for privilege and access management in higher ed, with three primary goals:

1. **Documentation**. As we have learned from past experience, it is important to focus on solving real-world rather than solely theoretical problems, and in order to maintain that focus, having a compendium of documented use cases to which to refer may be helpful.
2. **Categorization**. While use cases in this space originate in disparate parts of our organizations, we believe that common properties exist which can allow for categorization of use cases across functional areas. This may mean that many seemingly dissimilar user cases admit of solution with similar solutions, suggesting the potential for development of reproducible and reusable solution patterns for privilege and access management.
3. **Communication**. A use case library can provide a kind of shorthand for discussions of the problem space - rather than recapitulating entire use cases, some of which are complex and nuanced, we can simply refer to shared examples from the library. Further, by couching use cases in the terms their originators (who are typically focused on function rather than technology), we may facilitate communication with potential consumers of our work products.

<<Gartner text forthcoming, TBD>>

Since the 2009 CAMP, a number of additional use cases (some far richer than those originally collected) have been added to the collection. In the tabulation below appears the complete set of use cases collected to date with "user stories" where they are available, and with links to more complete documentation where appropriate. The cases are ordered according to their functional areas of origin (business cases, academics and research, etc.). Each case is associated with a letter and number (B-1 for the first business use case, or M-3 for the third medical center use case, for example), as well as two short names - one describing the use case in functional terms and one describing the use case in more technical terms. Space is provided in the table for additional information, including categorization and possible rearticulation using standardized language (XACML, etc.). Space is reserved for ad hoc tags, to facilitate identification of use cases related in ways not apparent from the simple titles and categorizations.

Use Case Library

Number	Functional Title	Technical Title	User Story	Categorization	XACML Representation	Further Documentation (links)	Source	Tags
B-1	Shared Budget Access by Director and Assistant	Delegation of Limited Budgetary Authority by Organizationally Identified Authority	Sarah is the new Director of Facilities Management. As the Director, she has the authority within the institutional ERP system to manage the access rights afforded to other individuals with respect to fund codes within Facilities Management. The Director wishes to have her administrative assistant process monthly budget reconciliation statements for her non-salary fund codes, but wishes to manage her salary fund codes directly. She explicitly grants her administrative assistant access to read and reconcile transactions against her non-salary fund codes in the ERP, but leaves herself as the sole individual with access to her salary fund codes.	Single organizational authority delegating multiple privileges to single subject by fiat			Duke	scope: organizati on, fund code type
B-2	Old and New Payroll Clerks	Position-based Role Reassignment in Payroll System	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 organizational authority transferring constrained privilege delegations between subjects by reconfirming roles		Proposed Solutions: Grouper, perMIT, Rice, Spocp	Duke	scope: organizati on, exempt /non-exempt
B-3	Clery Notifications While On Vacation	Temporary delegation of Approver Rights in Emergency Notification System	Richard is the institutions Vice President of Public Safety, and as such, he is authorized within an emergency notification system to approve Clery Act notifications which will be sent via multiple venues to the entire campus community. Richard schedules a two week vacation in Europe. He delegates his Clery role to the Chief of Campus Police, Trish, during his two week absence, allowing her to approve Clery notices in his stead. When a pair or armed robberies is reported outside a student dormitory one week later, Trish is able to approve a Clery notification for distribution on Richard's behalf. Upon his return from vacation, Richard revokes the delegation of his Clery role, and Trish loses her ability to approve Clery notices in the system.	Time-limited delegation of application privileges from authority to designee with a pre-defined time limit			Duke	scope: time-interval
B-4	Wellness Program Participation	Self-Service Enrollment in HR Program	A university's HR department offers a health and wellness program for university staff and faculty. The program is entirely voluntary. Participation requires a commitment by the employee to engage in a short online health awareness exercise, in return for which the university offers participants discounts on services at the university health club as well as periodic special offers from area business deemed by the university to be offering wellness-supporting services. A new employee in the physical plant hears about the program during an HR orientation and visits a web site to sign up. Once enrolled in the program, the employee has access to the program's web portal and receives weekly email reminders about training opportunities and special offers.	Self-service opt-in for multiple federated services constrained by affiliation with prerequisites.			Duke	n/a
B-5	Travel Reimbursement Approvals	Organizational Workflow for Expenditure Approval Driven by Organizational Hierarchy	Business rules within a college require that travel reimbursements in excess of $1,500 per diem be approved by the traveler's immediate supervisor or someone in the supervisor's management chain **and** countersigned by an agent from the college's Accounting office. Martha, the Assistant Director of International Relations, returns from a business trip to Switzerland and files a travel reimbursement form attesting to $1,800 in expenses on the final day of the trip. The reimbursements system routes his last day's request to the Director, who approves it in the system. The system then routes the approved request to the Accounting office, where it is checked by a member of the Accounting office's travel reimbursements team. Only after the expense report is authorized by the Accounting office does the system issue a reimbursement check to Martha for the $1,800	Hierarchical, subject-relative distributed workflow; multiple approval authorities designated by business role and organizational hierarchy			Duke	scope: spending limit
B-6	Housekeeping Access to Services	Automatic Provisioning to PTO Scheduling Service	The Housekeeping Office decides to do away with their legacy paper-based PTO (Paid Time Off) tracking system and begin using an online PTO system managed by the central IT group on campus. The new system provides, among other features, a combined calendar view of staff time off, holidays, and major campus events (so that employees may make more informed decisions about vacation scheduling). The system accesses group information derived from authoritative sources in HR and Payroll to associate individuals with their departments, and grants access to department-limited views of the combined calendar to all employees in each department. When Housekeeping begins using the online system, staff in the department are automatically granted access to a Housekeeping view of the combined calendar, listing the schedules of employees in Housekeeping along with University-wide events and holidays. As new employees arrive in the department, they are automatically added to the appropriate departmental group and gain access to the departmental calendar in the PTO system.	Automatic provisioning and deprovisioning based on organizational affiliation with organizational hierarchy-based privilege constraints			Duke	scope: organizati on
B-7	Enforcing Compliance Training	Institutional Continuing Education Requirements Enforced Through Scheduled Testing and Attestation	The University Compliance Office requires that all employees in specific job categories identified as having potential interaction with sensitive financial information (such as employee bank routing information or staff payroll information) complete an online training module on current procedures for securing sensitive information and attest to their agreement to follow documented University regulations. The system stores information in the institutional identity management repository indicating the date when an employee last completed the online training module, and periodically sends notices to individuals whose training is more than one year out of date and who still work in covered job categories. The training system grants access to the module automatically to employees whose IdM data indicate that they meet the criteria for completing the instructional module. Other applications that traffic in sensitive financial information include the currency of employee's training when making authorization decisions.	Organizational affiliation-driven time-limited entitlements with automatic renewal and prerequisites			Duke	scope: time interval

B-8	Trustee's Conflict of Interest	Limited Revocation of Privileges to a Trustee to Avoid Conflict of Interest	The Trustees share access to a secure wiki site where information regarding major capital projects being undertaken by the University is housed and discussed. One member of the board notices that in an upcoming meeting there will be a discussion of possible plans to sell some University land at auction to raise funding for a new building project. As a member of the local zoning commission, the Trustee must recuse himself from the discussion. The University secretary explicitly revokes the Trustee's access to the specific portion of the wiki related to the discussion of the real estate transaction in order to avoid any appearance of conflict.	Role-based Privilege Explicitly Revoked by Authority Without Affecting Role Due To Special Circumstances			Duke	scope: excluded document
B-9	Terminating Access for Disgruntled Employee	Emergency Revocation of Access Rights Due to Potential Security Risk	A Systems Administrator in the Computer Science department is terminated abruptly for egregious violation of University harassment regulations. When the employee is terminated, University policy states that his access to core services and systems must be terminated within 48 hours, and automated processes are in place to ensure compliance with that policy by removing the employee's access to systems throughout the institution. The automatic processes are triggered as overnight batch processes in order to avoid possible service interruptions during normal business hours. The Chair of the CS department, however, has reason to believe that the terminated employee may intend to do some mischief before his access is disabled, so to protect departmental systems, he contacts the IT Security Officer (ITSO) and requests an exceptional authorization change. The ITSO logs into a privileging system and, using rights granted to him by his functional role as ITSO, places an administrative block on all privileges afforded to the terminated employee, and triggers an immediate update of access rules on core systems and CS Departmental systems. Three hours later, the terminated employee attempts to log into the CS department's mail server and delete his accuser's account, but is denied access due to the ITSO's manual override. Overnight, the nightly batch run removes the user's access rights in all systems, making the ITSO's manual override unnecessary. The next morning the ITSO removes his manual override from the system.	Role-based Automated Privilege Management With Temporary Manual Override for Emergent Situation			Duke	Scope: range of privileges
B-10	Special Access for New Employee	Access to Programming Resources Delegated By Manager Based on Work Assignment	A new software engineer is hired by the Administrative Computing group. His addition to the staff automatically provisions him with an electronic identity and with access to some common productivity tools, etc., shared by all staff members. On his first day at work, his manager logs into an access management interface and adds the new employee to a group constructed to identify programmers working on a new Purchasing system. This automatically provisions with the new engineer with read access to the code repository for the Purchasing system, but does not automatically grant him write access to the repository. The first time the new engineer attempts to commit changes to the code repository, a workflow is triggered which notifies the project manager overseeing the coding project. The project manager reviews the new engineer's credentials and his attempted change, and determines that the new engineer should be granted commit rights in the repository. Once the project manager authorizes his commit rights, the new engineer is able to modify code within the Purchasing system.	Role-based Automated Privilege Provisioning Enhanced with Management-driven Manual Privileging			Duke	n/a
B-11	Budget Approval Process	Substitute Approvers Following Organizational Hierarchy in Budgeting System	A University budgeting system implements an hierarchy-based policy for budgetary approvals, in which budgets for organizational subunits are submitted by their respective managers and approved by their department heads, who in turn submit their combined budgets (along with their own offices' discretionary budgets) for approval to school or divisional managers, who in turn pass their combined budgets to senior administrators and ultimately to the CFO for approval. The scope of budget approval authority granted any given manager in the system is controlled by the organizational unit the manager is charged with overseeing. The authority who must approve any given manager's budget is dictated by the organizational hierarchy, which is represented in the system with hierarchical groupings of subunits, departments, and divisions. In the event that a given approver is unavailable for any reason, any authority at a point closer to the top of the hierarchy may issue approvals in his or her stead. When the Director of Transportation is out on childcare leave during budget finalization, it falls to the Assistant VP of Auxiliaries to approve both the Director's discretionary budget and the budgets of her subordinate managers for the Parking Office, the Campus Transit Authority, and the Traffic Control Office.	Hierarchical Roles Followed by Automated Approval Process to Compensate for Subject Unavailability			Duke	scope : organization
B-12	Budget Approval for New Department	Unconfigured Fallback Approvals for New Department in Budgeting System	At that same University, the budgeting system eventually encounters a new interdisciplinary program in Genomics that comprises faculty and staff from a number of different departments spanning multiple schools and colleges. The Program Director submits budget into the system, but since the program is not part of any officially recognized school or division, the Director's budget is routed all the way to the Provost for approval.	Hierarchical Roles Followed by Automated Approval Process in the Absence of Explicit Delegation			Duke	scope: virtual organizations
B-13	Employee RIF	Temporary Access to HR Resources for RIF'd Employee	An employee is separated from the institution due to a RIF (Reduction In Force) in her department. HR rules require that she retain access to the campus HR portal and to career development resources for 90 days following her separation to facilitate her transition into a new position (whether internal or external). The campus access management system notices her separation and removes her from all active employee groups and roles, thus denying her access to most staff-accessible systems on campus. She is automatically granted specific access to the HR portal and the career center library system for 90 days. At the end of the 90-day grace period, her rights in those two systems automatically expire.	Temporary Automatic Role Assignment Based on HR Termination Policy			Duke	scope: time interval,
B-14	Inappropriate Purchase with Institutional Funds	Audit Logs Used to Identify Impropriety in Purchasing System	An incident involving the possible misuse of a University purchasing card to acquire an item of jewelry is being investigated by Internal Audit. The investigator requests a report from the purchasing system of when and by whom the specific purchase was approved, and finds that the purchase was approved by an administrative assistant with authority to approve purchases only up to $500. The investigator then retrieves a report from the access management system of all privileges previously assigned to the administrative assistant, and finds that on the date the purchase was approved, the employee was granted approval rights up to $5,000 for a period of four hours. The investigator notes in the audit log that the assistant's manager - the Assistant Director of Finance - had granted those rights to her. After further investigation, it is determined that the Assistant Director had granted those rights to her assistant in violation of University regulations, and had then directed her to approve the purchase in an attempt to avoid its being detected by the auditors. Both the Assistant Director and her assistant undergo disciplinary action as a result of the incident.	Privileging State Logs Audited for Point In Time Privilege Review			Duke	scope: time interval, spending limit

B-15	Affiliation Transitioning	Full-time staff /Part-time Student Transitions to Full-Time Student	A staff member in the Accounting office applies for admission to the graduate program in Mathematics and is accepted. Three months into her graduate program, she decides to vacate her position in Accounting and become a full-time graduate student. When she transitions out of her Accounting position, her access rights to the university ledger and other financial accounting systems are revoked automatically, but as a continuing student, her university ID, her university electronic identity, and her common services accounts (email, scheduling, collaborative applications) remain active, as do her student services (access to the campus LMS, access to the Bursar's bill tracking system, etc.).	Automatic Recalculation of Privileges based on Granular Changes in Multiple Affiliations			Duke	n/a
A-1	Off-Campus Colleague Access to Local Research Results	Inter-Campus Collaboration Between Genetics and Pharmacology	Professor Smith, of the Department of Pharmacology in the Medical School, is researching the chemistry of snake venom to determine whether certain components of various snakes' venom may be useful in the management of chronic pain. Professor Jones, in the Department of Genetics, has recently completed a mapping of the genome of one particular species of cobra, and after reading an article by Professor Smith on that cobra's venom, offers to share his research results with him. Professor Jones explicitly grants access to his cobra genetics notes in the Genetics Faculty wiki to Professor Smith, who uses Professor Jones' research to further his analysis of the components of the particular cobra's venom.	Single Resource Owner Delegating Multiple Privileges to Single Subject by Fiat			Duke	scope: wiki-objects? or none resource could specify a URL
A-2	Adding a Lab Assistant	Faculty Designating Lab Assistants in an LMS	A faculty member in the Department of Physics arranges to have one of his better undergraduate students from the previous semester act as a lab assistant for his structural dynamics class. He adds the "lab instructor" role for Physics 108 to the student's profile in the learning management system (LMS) and the student automatically gains access to lab teaching materials and student lab reports for the course.	Single Authority Explicitly Assigning Application-specific Role to Single Subject by Fiat			Duke	n/a or scope is class-identifier (student-id, read, teaching-materials, class-id) or (student-id, read, class-id, (teaching-materials, lab-reports))
A-3	TA Grade Access	Delegated Gradebook Access in LMS for Teaching Assistant	A university uses its LMS to handle mid-term grade reporting - faculty enter grades for assignments and mid-term quizzes and exams in the LMS, where students can review them online and track their progress until the end of the term. The LMS automatically assigns grade entry privileges to instructors (as identified by the student registration system). Professor Gamow chooses to have one of his graduate students act as TA for his EM Fields course and delegates his grade reporting privileges in the LMS to his student. The student is then able to report grades for students in the EM Fields class within the LMS. When final grades are due, Professor Gamow reports them to the Registrar based on information previously reported in the LMS.	Single Authority Explicitly Assigning Application-specific Role to Single Subject by Fiat			Duke	??
A-4	Resource Owners Managing Access Data	Delegated Administration of Privileges for Departmental Administrators	A university's central IT organization operates an authorization service used by all its colleges and schools to manage access rights within a shared faculty management application. Central IT staff find themselves spending increasing time entering role and permission changes on behalf of the schools. Central IT staff use a delegation mechanism built into the authorization facility to grant administrative staff in each School direct access to authorization rules for resources within their Schools, relieving them of workload and distributing decision-making authority to resource owners.	Central Authority Delegating Organizationally-scoped Privilege Management Capabilities in Central Privileging System			Duke	scope: school (organizati onal)
A-5	FERPA Information Restricted	FERPA-Compliant Opt-out of Directory Publication	Under federal regulations, certain educational records information about students may be categorized as "directory information" and may be disclosed by institutions without prior consent from students. Students reserve the right under FERPA, however, to have disclosure of their directory information blocked upon request. An undergraduate Engineer becomes concerned that a high-school acquaintance may be stalking her, and wishes to have her contact information (name, address, email address, telephone number) blocked from view. The university considers those data elements to be directory information under FERPA, and discloses them by default. The student visits a FERPA portal system and marks those data elements as FERPA protected information in her records. Subsequently, applications that access student educational information and IdM data about students refuse to allow access to the student's contact information except when the requester is identified as having an academic need to see the information.	Subject-specific Opt-In Privilege Override for Compliance with Federal Regulations			Duke	scope: student-record-id, student-attribute-id
A-6	Course Registration Exceptions	Registration Approval Required Based on Student Career /Major	A Biomedical Engineering (BME) student in her senior year signs up for Professor Jones' popular seminar on biomedical research ethics. As a BME upperclassman, the registration system allows her to sign up directly. Her roommate, a pre-med student majoring in Public Policy, attempts to sign up for the same course, but because of rules applied to the course in the registration system, the second student's registration for the course is suspended, and the system sends an approval report to Professor Jones. Having spoken with the student beforehand, the professor is prepared for the request, and authorizes it in the registration system. The pre-med student is enrolled in the class.	Single Authority Acts as Approver Overriding Subject-based Access Policy via Workflow			Duke	(student, can-enroll, class-id) ((student-group), can-enroll, class=id) ((student-group), can-enroll, (class-group))
A-7	Restricted Blog Access	Professor Granting Access to Personal Blog for Course Registrants	Professor Pilkey wants to grant access to a blog he maintains about his research into the effects of pollution on shallow-water marine invertebrates to students in his Wetlands Ecology course. The campus IdM system automatically places students in course-specific groups based on their enrollment in specific sections of specific courses. The blogging software supports LDAP-based groups, so Professor Pilkey grants access to his blog to the members of the "ECO 212 Students" group.	Automatically Managed, Attribute-Driven Group Membership, and Single Authority Delegating Access to Single Resource to Derived Group			Duke	

A-8	Course Deadline Extended	Single Student's Access to LMS Extended due to Approved Absence	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.	Single Authority Explicitly Granting Time-limited Access Previously Granted Automatically via Group Membership to Single Subject		Proposed Solutions: Grouper, perMIT, Rice, Spocp	Duke	scope: time-interval
A-9	Career Services	Identity-based Access to Career Counseling Resources	Career Counseling Services arranges to have an online course in effective interviewing techniques made available to students who meet specific criteria - those who are expected to graduate within one year and who are in degree-seeking programs (part-time and inter-institutional students are excluded). The vendor providing the online course materials requires that the center make a good faith effort to limit access to those students. The center arranges to grant access to any student whose expected date of graduation is less than one year in the future and whose identity information indicates she is a full-time student.	Rule-based Access Control Employing Multiple Identity and Time-dependent Attributes			Duke	scope: expected-graduation-date ((student-group), access, online-course materials, expected-graduate-date)
A-10	Adding TA Access to Course Dropbox	Special Access to "Dropbox" Area in Shared Filespace for Designated TAs	In a shared filespace, a faculty member desires to grant read access to course materials to both his students and his TAs, write-only access to a dropbox or his students, and read-only access to the dropbox for his TAs. The file server consumes group information from the identity management system to enable the faculty member to grant read to the course materials for his students, but because only the faculty member knows the identity of his TAs, he manually adds the TAs one by one to an access whitelist for the shared filespace.	Single Authority Employing Whitelist with Centrally Managed Group Memberships to Manage Access Rights in Shared Filespace			Duke	
A-11	Faculty Survey Access	Special Access for Internal Pedagogical Research	A faculty member in Education working for the Provost's office on a multi-year effort to enhance undergraduate instruction is researching the effectiveness of different pedagogical strategies in the treaching of new foreign languages to non-language majors. He develops a survey which he wants instructors teaching introductory language classes in all foreign language departments to respond to. He grants permission to access the survey to faculty members and graduates students identified as instructors in at least one section of a 0-level foreign language course. The Registrar later grants him access to depersonalized grade information from 0-level foreign language classes to complete his research.	Single Authority Delegating Access Based on Transient Roles; Single Authority Explicitly Assigning Limited Access by Fiat			Duke	
A-12	Approval of Faculty Promotions	Hierarchical Access to Faculty Activity Records for Tenuring and Promotion	A web-based faculty management and promotion system needs to grant access to faculty CVs and evaluations in a way that reflects the institutional academic hierarchy. Professor Jones is both an instructor in the department of Microbiology and the Chair of the department. As a department chair, Professor Jones has access both to his own CV and to the CVs and evaluations of all faculty within the department. Professor Johnson is the Dean of Basic Sciences, and teaching faculty in the Anatomy department. Because Microbiology is part of the Division of Basic Sciences, Dean Johnson has access to professor Jones' CV and evaluation reports, as well as to all the CVs and evaluations of faculty in Microbiology and other departments within the division. She has access to her own CV as a faculty member, but not to the CVs of faculty in other parts of the School of Medicine. Dean Hillard is the Dean of Medicine, and has access to all faculty information in the School.	Multiple Authorities Sharing Role-based Access Scoped Based on Organizational Hierarchy			Duke	
A-13	Access to Course Resources	Faceted Access to Course Spaces in Shared Filesystem	Professor Hausmann teaches four sections of Basic Anatomy in the Medical School, one of which is cross-listed in Comparative Biology and co-taught by Professor Biggs. In conjunction with an LMS system, the university provides shared filespace for instructors to use in their courses. By default, instructors are given one shared directory for each course they teach and one subdirectory for each section of each course. Professor Hausmann is granted full privileges in a top-level shared directory for his Basic Anatomy course (BA4401) and in subdirectories for each of the four sections of the cours (BA4401S1 thru BA4401S4). Students in each section are given read access to the BA4401 directory and to their individual sectional subdirectories, but not to other sectional subdirectories. Professor Biggs is automatically granted full access to the BA4401S4 subdirectory, which is also referenced through a filesystem link as CBIO410S1. Students enrolled in the cross list have access to the one subdirectory and the BA4401 super-directory.	Multiple Subjects Share Privileges in Hierarchical Filesystem Mapping Pedagogical Hierarchy			Duke	
A-14	Requisite Training for Lab Access	Safety Certification Required for Physical Access to Laboratory	A new graduate student matriculates in Biochemistry and as a result is granted card access to the Chemistry and Biology buildings and all departmental areas except a Class 2 pathogen lab in the basement of the Biology building. Access to that lab is contingent upon completion of a rigorous course in safe handling of Class 2 human pathogens and the operation of the labs safety equipment. The graduate student completes the course a week after matriculation and once the occupational health and safety office updates his IdM information to indicate that he is in compliance with the requirement, his card grants him access to the lab automatically. Six months later, his compliance comes due for renewal, and he's notified that he must complete a refresher course to continue his access to the lab. Having completed the only course involving use of the Class 2 lab he plans to take, he chooses not to renew his certification, and as it lapses, his card access to the lab is revoked.	Automatic Prerequisite Certification Processing for Physical Access Control			Duke	scope: time-interval

A-15	Student Registration Glitch	Temporary Access Failure Due to Automated Registration Glitch	Professor Stedman's Marketing 304 course culminates in a final project which is to be submitted electronically by each student no later than 5pm on the last day of class. A student in the class fails to submit his final project on time and reports that he was denied access to the class dropbox when he attempted to submit his assignment. The instructor is suspicious and retrieves audit logs from the LMS which indicate that the student was indeed denied access to the dropbox at 4:45 on the appointed day. Enlisting the assistance of his IT support staff, Professor Stedman finds that the student was removed from the Marketing 304 Student group that morning, and reinstated in the group the following morning. Further investigation by the IT staff determines that a failure in the university registration system had caused truncation of the student list for Marketing 304 and caused the student in question to be errantly reported as not enrolled in the course for approximately 24 hours. In light of these facts, Professor Stedman grants the student an extension and allows the student to submit his final project for full credit.	Single Authority Authorizing Rule Variance Based on Forensic Evaluation of Audit Trail			Duke	
A-16	Colleague Submitting Grades for Another	Substitute Grade Submitter Designation in Registration System	Professor Jones in the School of Engineering is planning to attend an IEEE event in Switzerland and will be unavailable for three weeks at the end of the semester. She has arranged to have final grades for all of her students completed prior to her departure, but due to restrictions set by the Registrar's grade reporting system, she can't enter the grades officially until after the semester ends. She arranges for a colleague (Professor Wilson) to enter her grades for her, and in order to enable this, transfers her rights with respect to her Signals course to her colleague, limiting the transfer to the specific range of dates during which she will be in Switzerland. When the time comes for grade reporting Professor Wilson is able to post Professor Jones' Signals grades on her behalf. Three weeks later, Professor Wilson accidentally attempts to open Professor Jones' grade report for her Signals class and is denied access by the grading system, since Professor Jones' transfer of authority has expired.	Time-limited Delegation of Privilege by Single Authority to Single Subject			Duke	
A-17	Pre-Hire versus Post-Hire Affiliation	Pre-Hire Identity Creation and Interim Role Assignment for New Faculty	Normal HR processes ensure that new employees and faculty are automatically provisioned with electronic identities and granted appropriate access to services based on their roles within the organization on the morning of their first official day at work. Dr. Zalib Bentha is the world's foremost authority on the lasing behavior of gallium-based solid-state lasers, and has just accepted a position in the Electrical and Computer Engineering department at the University. His effective date in the position is six months hence, but because of the importance of his hiring to the School of Engineering and his interest in beginning to build collaborations before his arrival, the Dean of the School makes an urgent request to have soon-to-be Professor Bentha provisioned for access to the University e-mail system and the School's collaborative wiki system. Staff in the electronic access management group follow a pre-defined procedure to enroll Dr. Bentha in the University identity management system as a special "pre-hire affiliate". He is automatically issued an electronic ID, but is not populated in any specific user groups. His pre-hire status grants him automatic access to and provisioning for the University email system, but does not give him access to departmental resources. As part of the pre-hire workflow, the Dean's office is notified when Dr. Bentha's identity is created, and staff in the Dean's office explicitly grant him access to the Engineering wiki system. Six months later, when Professor Bentha begins his tenure at the school, the normal HR process adds him to various faculty groups and removes his pre-hire affiliate status and associated "special" privileges. The Professor arrives on his first day in the department and sees no interruption in his existing access to services.	Explicit Assignment of Limited-Access Role Subsequently Superseded by Automated Role Assignment			Duke	
A-18	Delegated Directory Administration	Delegated Management of Objects and Privileges in a Directory Based on Departmental Hierarchy Within a School	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.	Hierarchical Delegation of Administrative Privileges Mapping Organizational Hierarchy; Role-based Access Rights Scoped by Departmental Affiliations		Proposed Solutions: Grouper, perMIT, Rice	Duke	

A-19	FERPA overrides for IT support staff	Limited Delegation of Privileged Access to IT Support Staff Based on User Attributes	A University's Registrar has determined that student cell phone numbers are privileged directory information under FERPA, and as such, can be blocked from access except in cases of academic or other demonstrated business need. Cindy is a Junior in the Music department, and is concerned that an acquaintance from her high school may attempt to harass her if her cell-phone number is made public. She uses the campus student information system to assert her privacy rights under FERPA, marking her cell phone number as unpublished. Later, Cindy decides to enroll in an SMS messaging service on campus that will allow her to receive emergency notifications on her cell phone (as well as via electronic mail and other means). A month after she enrolls in the SMS service, a weather emergency results in notifications being sent by the University to all enrollees, and although she receives notice of the emergency through the campus email and IM systems, she fails to receive her SMS message. She calls the campus IT Service Desk, where Jorge, a help desk analyst, answers her call. Jorge opens a directory search tool and searches for Cindy's directory information. Normally, since her cell phone number is listed as FERPA protected, Jorge would not be able to access it, even though he is a member of a security group granted access to cell phone number information that isn't constrained by FERPA. Since he is recognized as a technical support analyst, and since Cindy's records indicate that she's enrolled in the SMS notification service, Jorge is able to see her registered cell phone number, and is able to determine that she mis-reported her cell number during enrollment in the notification service. Cindy is able to return to the SMS notification sign-up web site, corrects her cell phone number, and receives the next emergency notification sent by the University on her SMS device.	Data Access Constrained at Authorization Time by Attributes of the Subject Being Acted Upon; Real-Time Constraint Evaluation			Duke	Real-Time Evaluation scope: emergency-notification-active
A-20	DUS Student History Access	Privileged Access to Student Records by D. U.S. Based on Major Declaration	A College institutes a privacy policy under which student grade history is considered confidential information that can only be accessed by individuals with a demonstrated need to see it. The Registrar interprets the policy to mean, among other things, that faculty should have access to student grade history only on a "need to know" basis. She declares only two such "need to know" cases _a_priori_: pre-major advisors assigned to individual students should have access to their charges' academic histories, and Directors of Undergraduate Studies should have access to the academic histories of students who are currently majoring in or who have declared concentrations in their respective departments. Nikolos is a second-semester Sophomore Physics major who, during drop-add period at the start of the Spring semester, decides to change his major from Physics to Mathematics after encountering his first Thermodynamics course. The afternoon after he enters his major decision into the campus student records system, he visits Prof. Bessel, Director of Undergraduate Studies in the Mathematics department. During their discussion about the Math program, Dr. Bessel logs into the student information system and is able to review Nikolos' academic history. He points out that Nikolos is enrolled in a non-majors differential equations course, and after evaluating Nikolos' grades in his introductory calculus and multivariate mathematics courses, determines that his high marks make him an excellent candidate for enrollment in Prof. Leibnitz's introductory seminar on differential equations for Mathematics majors. Nikolos adjusts his schedule before the close of drop-add and enrolls in Prof. Leibnitz's seminar. Later, Prof. Thorpe, Director of Undergraduate Studies in the Physics department, hears that Nikolos has decided to change his major, and attempts to review his grade history for some indication of his possible reason for making the change. He is surprised to find that he can no longer access Nikolos grade history in the student information system, since Nikolo is no longer listed as majoring in Physics, and makes a note to contact Nikolo directly to discuss his decision to change majors.	Data Access Constrained by Authorization-Time Evaluation of Attributes of the Subject Being Acted Upon; Real-time Constraint Evaluation			Duke	Real-Time Evaluation
A-21	Extended file system space for LMS Mastered Classes	Delegated control of file system quota to instructors and TAs with access changing as external events are declared	Many of the classes represented in the LMS require large amounts of file storage be allocated and maintained for digital artifacts. File storage is assigned to the faculty member teaching the class, Professor Charles Xavier. Xavier and his teaching assistant Scott Summers assign this file storage to the 20 students in the class and to mission teams in the class. Mission teams reflect assignments and projects. Charles and Scott also allocate some of the file storage to reference materials for the class as a whole. The file storage that contains reference material is readable by Xavier and Summers and all members of the class. Xavier and Summers can also write and delete the reference material. The file storage allocated to individual students has read/write/delete privileges for the student and read privileges for the faculty member and TA. Xavier and Summers assign students to mission teams for each of three missions that occur during the class. For example of the 20 students in the class each may be assigned to 1 of 4 mission teams that exist concurrently. Each mission receives file system quota where each mission member has read/write/delete privileges and Xavier and Summers have read privileges. At the end of the mission team member loses the privilege to delete mission material and Xavier and Summers gain the privilege. When concurrent mission are all completed, the mission material is deleted.	Data Access constrained by delegation and external events			CMU	
RL-1	Special Access by Student Employees	Special Access in Housing Lottery based on Multiple Affiliations	The Undergraduate Housing office employs a small number of work-study students each semester as aides during the undergraduate housing lottery. Their job is to enter information from paper forms submitted during the lottery process by other students into the online room assignment system. Under normal circumstances, first-year students are blocked from accessing the online room assignment system until the second week of the housing lottery in order to give upperclassmen priority for housing selection. Gina is a first-year work study student hired to work during the housing lottery in the Spring semester. A privileging system detects that while she is a first-year student, she has been designated a Housing employee for the three weeks of the lottery, and grants her early access to the room assignment application. Her supervisor takes responsibility for ensuring that she does not abuse her privileges to assign herself a room before it is appropriate for her to do so.	Role-Based Access Conflicts in Multi-Role Use Case			Duke	

ID	Title	Subtitle	Description	Pattern		Proposed Solutions	Institution	
RL-2	Dorm Access for Residential Advisors	Special Physical Access to Dorms for RAs	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	Role-based Access Control for Physical Access Scoped by Geography and Granular Role Status		Proposed Solutions: Grouper, perMIT, Rice	Duke	
L-1	Temporary Privileges for External Patrons	Special Access to Rare Book Room for Local Historian	Jake is an art historian living in town and working for a local art dealer, where he authenticates 18th century paintings for the dealership. The University library happens to have in its rare book holdings the most authoritative reference (written in the 1880's) on the works of an obscure Viennese artist of the mid 1750's, one of whose better-known works is being offered at auction. Jake suspects that the painting may be a forgery, but needs to verify some facts in the authoritative reference. He contacts the University library, and finds that while the library is pleased to offer on-site access to its public stacks to causal patrons, access to the library's rare book room is more constrained. Jake visits the library's reference desk and is issued a temporary patron card. The reference librarian adds the patron ID associated with the card to a rare book reader group through her desktop client. Jake uses the card to access the rare book stacks, and is able to find that in fact the painting is authentic. When he returns his temporary patron card to the reference desk later in the day, the reference librarian revokes that patron ID's rare book access privileges.	Single Authority Explicitly Grants Physical Access to Transient Identity Via Group Membership			Duke	
L-2	Professional Organizations and Federations	Inter-Library Association Federates Access to Electronic Resource	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).	Federated Identity Coupled with Federated Group Membership Information for Shared ACcess Control		Proposed Solutions: Grouper, perMIT, Rice	Duke	
L-3	Anonymized Access to Resources	Privacy-Protecting Federated Identity in Access to Sensitive Library Resources	Another librarian at the same institution is establishing a new collection of electronic documents pertaining to recently declassified information about the US response to terrorism during the late 20th century. The artifacts in the collection are to be made available for online interlibrary access to faculty and graduate students at colleges in the tri-state area surrounding the university. Although the material is declassified, there is significant concern about the privacy of individuals who may wish to access it. The university participates in an identity federation that encompasses the tri-state area. The librarian arranges to have access to the new electronic collection protected by a federated identity system that allows patrons to authenticate at their "home" institutions within the federation and access materials at the university. He arranges to request only the necessary information about patrons from their home institutions - scoped affiliation information sufficient to distinguish between students and faculty at participating institutions and other individuals, but not sufficient to identify the individuals uniquely, thus protecting the anonymity of users without allowing unauthorized access to the collection.	Attribute Release Policy Limitations Protecting Anonymity in Federated Library Access Model			Duke	
M-1	Chart Access by Consulting Physicians	HIPAA-Controlled Access to Patient Records for Physician During Consult	Hospital rules interpret HIPAA privacy regulations to dictate that only those medical staff and faculty directly involved in the care of an individual patient should have access to view that patient's medical records during treatment. Faculty in the medical school may have access to depersonalized medical data for purposes of research and instruction, but may only view personally identifiable medical information if referred a patient by an attending physician. An attending physician in the ER is treating a patient with symptoms of West Nile viral infection, and needs a consultation from an Infectious Disease specialist in the Medical School. The attending instigates a consultation and referral process which grants the ID specialist temporary access to view the patient's medical records. Once the consultation is complete, the ID specialist's access is revoked automatically.	Temporary Delegation of Access Rights Based on Transient Role Assigned by Single Authority			Duke	
M-2	Nurse Changing Departments	Rights Management for Itinerate Nurses in Multiple Wards	Patient care needs require that all nurses working in Orthopedics have access to Ortho patients' medical records. When Nurse Mills moves from the day shift in Physical Therapy to the night shift in Orthopedics, a nursing supervisor adds the "Ortho Nurse" role to her profile in the medical records system, granting her appropriate access for her new role. The shift supervisor in PT likewise removes the "PT Nurse" role from her profile, removing any rights she was granted during her time on the day shift. When Mr. M. is admitted to Orthopedics after presenting in the ER with a fractured pelvis, his admission to Orthopedics automatically grants Nurse Mills access to his medical records.	Granular Roles Assigned by Single Authority Based on Work Assignments; Automatic Role-based Access Scoped by Subject Identity			Duke	
M-3	Drug Restocking Approval	Automatic Approval Chain for Scheduled Substance Refills	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.	Automated Workflow Driving Multiple, Ordered Authorizations for Restricted Operation		roposed Solutions: Grouper, perMIT, Rice	Duke	

M-4	New Nurse Access /Onboarding	Temporary Privileges Granted to New Nurse in Emergency	Sarah is in the process of being onboarded as a new nurse in the Emergency department when a major industrial accident is reported in the area. Since the university medical center is the main trauma center for the region, an "all hands" call is placed for emergency medical staff to handle the expected increase in patient volume. The new nurse is on-site and prepared to provide support, but the university privileging system has not yet activated her access to hospital records and pharmacy systems, pending a scheduled overnight batch process. The head nurse on duty in ER logs into the privileging system and explicitly grants temporary access to both systems to Sarah, overriding the normal system workflow. Later, when the batch process executes, additional privileges are afforded to the new nurse in keeping with her position, and the head nurse's override is removed.	Explicit Assignment of Limited-Access Role Subsequently Superseded by Automated Role Assignment			Duke	
G-1	Temporary Network Access for Guests	Guest Network Access for Visiting Faculty, Affiliates	A university offers wireless access to all its official affiliates through a web-based registration system that requires authentication against the institutional SSO system. A number of non-traditional affiliates and guests, however, need to be granted access to the wireless network during their stays on campus, but since they are not tracked by the central university identity management system, they cannot use the wireless registration mechanism. A separate application is devised that allows specific individuals within recognized "gateway" units on campus (the Library, the International House, the Faculty Club, and the Office of Residential Life) to authorize guests for special guest access to the wireless network. These individuals act as registrars for the guests they authorize, registering them in a guest access system. The web interface allows registrars to review, add and remove guests from their lists of "approved" guest network users. The guests then have access to an alternative web interface that allows them to register their wireless devices for access via the guest wireless network.	Multiple Designated Authorities Delegating Controlled Access Rights to Multiple Unregistered Subjects			Duke	
G-2	Temporary Accreditation Committee Access	Temporary ID Provisioning for Institutional Accreditation Committee Members	An institutional curriculum committee is convened every five years by the Provost to review the curricula of the disparate Schools and make adjustments to align curricula with changes in institutional focus and/or new pedagogical goals and strategies. The committee meets in camera twice monthly for a 12 month term each time it is convened. Only the committee's final report is made public - minutes of its sessions and communications between the committee members are made available only to members of the committee, the Provost, and the Chancellor through a secure wiki. Every ten years, an external accreditation committee visits campus to conduct a review for the university's reaccreditation, and as part of its effort requires access to the minutes of the curriculum committee's meetings. The accreditation committee comprises faculty and administrators from a number of peer institutions, none of whom are affiliated with the university in other ways. Accreditation committee members are granted "ex officio" identities which are then granted access to the curriculum committee's meeting minutes in the secure wiki. The ex officio identities are revoked once the accreditation committee's final report is delivered.	Explicit Provisioning of Temporary Identities for Ex Officio Users			Duke	
V-1	caBIG Federated PI Access	Federated Access to caGRID Data Resources by a Principal Investigator	Dr. Simpson is an epidemiologist conducting research into pancreatic cancer at Duke Medical School. He is named principal investigator in a grant from the NCI under which genetic analysis of tens of thousands of tissue samples from malignant pancreatic tumors will be correlated with levels of benzene and related metabolites in the samples using caGrid resources distributed across the nation to investigate the relative contributions of benzene exposure and genetic predisposition to the eventual development of pancreatic cancer. During the research effort, Dr. Simpson wishes to retrieve data collected at a participating hospital in Oregon. Since the Oregonian hospital is participating through caBIG in the research study, its applicable tissue sample information is already exposed through various caGRID applications. Dr. Simpson accesses a caBIG portal application using his web browser, authenticates via Duke's Shibboleth IDP, and is recognized as his federated identity, "drsimpson@duke.edu". When he subsequently uses the portal to access the Oregonian hospital's tissue bank database, the Oregonian application is able to verify through the caBIG federation that "drsimpson@duke.edu" is the official PI for Dr. Simpson's pancreatic cancer study, and grants him access to the tissue data he seeks.	Federation or VO Providing Attribute Information Supplemental to a Subject's Primary Identity			caBIG	

| V-2 | Patient Referral Between caBIG Clinical Trials | Federated PIs within caBIG Sharing Resource Access to Refer Patients Between Clinical Trials Based on Trial-Specific Authorization Policies | Dr. Lister is an oncologist currently affiliated with the University of Chicago Medical Center. He specializes in the study and treatment of thoracic neoplasms including cancers of the lung and mesothelioma. He is currently the PI for a nationwide study investigating the efficacy of a new combined drug protocol in prolonging survival among stage 4 mesothelioma patients. His study relies upon caBIG resources distributed throughout the country for access to clinical results and to identify candidates for the study. Dr. Wong is an oncologist at the University Hospital of Arkansas, and is the PI for a nationwide study of the efficacy of a new radiological protocol at treating stage 2 and stage 3 thoracic and peritoneal malignant mesothelioma. At a caBIG colloquium in St. Louis, Dr. Wong attends a presentation by Dr. Lister in which he shows early results indicating that the combined drug protocol he is studying can significantly limit the progress of late-stage mesothelioma in patients whose disease has proved refractory to radiotherapy. After the presentation, Dr. Wong discusses the possibility of referring some of the patients in his epidemiology study whose malignancies have shown no clinically significant response to the trial protocol and have progressed beyond the limits of his own study to Dr. Lister for possible inclusion in his research study. They agree that some of Dr. Wong's patients would be appropriate candidates for Dr. Lister's sudy.

Six weeks later, Dr. Wong reviews the case of a participant in his study whose disease has progressed to stage 4 despite treatment with the test protocol, and decides to refer the patient to Dr. Lister's study. After discussing options with the patient, he logs into the caBIG clinical participant registry using his UHA credentials. As PI of his research study, he is able to immediately retrieve his patient's records, but he finds that he is not authorized to refer patients to Dr. Lister's study (although, as a PI in a caBIG-supported trial, he is able to access Dr. Lister's study information through caBIG workflow system and retrieve Dr. Lister's contact information from a directory of caBIG PIs). He contacts Dr. Lister by phone, and reminds him of their discussion in St. Louis. While on the call, Dr. Lister logs into a custom web application designed by his local IT staff and indicates that he would like mawongmd@uah.arkansas.edu to be authorized as a "referring physician" in his nationwide study. The application updates trial-specific authorization information at UCMC to indicate that Dr. Wong is now a referring physician in the Lister study. When Dr. Wong again attempts to refer his patient to Dr. Lister's study, he is successful. | Federated Identity Bound to VO-provided Role Attributes Scoped to Unique VO-Defined Contexts and Interpreted Through Context-Specific Policies; VO Participants Associated with Multiple Context-Dependent Roles by Relying Parties | | | caBIG | |