Rice KIM and selected uses 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.

The following illustrates how this use case might be modeled using KIM:

Principals

Mary is defined as principal entity in the KIM system.

Name	Principal ID	Entity Type	email address	
Mary	301	Person	mary@ucsd.edu	

Group Definitions

Suppose the following group has been defined to identify the students in Dr. Schonfeld's class.
Mary is a member of this group.

Group Type Name	Group Namespace	Group Name	Active	
CourseType	Academics	Students MATH20D Fall 2009	Y	

KIM Types

The KIM type identifies the set of attributes (fields)used to separate different instances of similar groups.
In this case, suppose the KIM type **"CourseType"** identifies the following attributes.

- Course
- Term
- Instructor
- Time
- Room Number

This separates these groups by course. For example: Dr. Schonfelds Ordinary Differential Equations course, Fall 2009,

Roles

For simplicity, this example is assuming that the LMS Role defines access to the LMS system. And that the authorization of specific LMS permissions are managed within the LMS system. KIM could be used to manage these LMS specific authorizations, but that is not illustrated in this example.

LMS User
Type: CourseType
Permissions:
. Login

Role Assignments:
Originally, the entire class was granted access by their group assignment:

Namespace	Role Name	Type	Member ID	Name	Active From	Active To	
Academics	LMS User	Group	MATH20D:Fall 2009: Students	n/a	09/02/2009	12/18/2009	

Use Case Action: To extend the student, the Professor can add a role assignment for the student that will expire in one week.

Namespace	Role Name	Type	Member ID	Name	Active From	Active To

Academics	LMS User	Group	MATH20D:Fall 2009: Students	n/a	09/02/2009	12/18 /2009	
Academics	LMS User	Perso n	301	Mary	12/18/2009	12/25 /2009	

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.

Actors in this use case:

- Gina, the current Chemistry payroll clerk.
- Marcus, the new Chemistry payroll clerk
- Sally, the Chemistry Payroll Supervisor

How this scenario might be represented by KIM:

Principals

Gina, Marcus, and Sally are all defined as principal entities in the KIM system.
As entities, KIM has various fields defined for each of them including

- Name
- Principal ID
- Primary Home Department Code

Name	Principal ID	Entity Type	Home Dept.	email address
Gina	100	Person	Chemistry	gina@ucsd.edu
Marcus	101	Person	Chemistry	marc@ucsd.edu
Sally	102	Person	Chemistry	sally@ucsd.edu

Group Definitions:

Suppose the following groups have been defined.

Group Type Name	Group Namespace	Group Name	Active
Departmental	Staff	Finance Admin Assistants	Y
Departmental	Staff	Executive Assistants	Y
Departmental	Staff	Business Officer	Y
Departmental	Staff	Department Chair	Y

KIM Types:

The KIM type identifies the set of qualifier attributes (fields). These qualifiers are used to separate different instances of types of group.

In this case, each of the above groups has a KIM type of "Departmental".
The Departmental Group Type defines a single attribute

- DepartmentCode
  This separates these groups by department. For example: Chemistry payroll clerks from Medical Center payroll clerks.

Group Assignments:

Group Assignments at the beginning of this scenario could be as follows:

Namespace	Groupname	Type	Member ID	Name	Active From	Active To Date
Staff	Finance Admin Assistants	Principal	100	Gina	6/30/1998	
Staff	Executive Assistants	Principal	101	Marcus	01/01/2009	
Staff	Business Officer	Group	Dept. Chair	--	04/01/1990	
Staff	Dept. Chair	Principal	102	Sally	10/10/2002	

Gina is assigned to the Finance Admin Assistants group.
Marcus is currently an executive assistant.
Sally is assigned as a Dept. Char and is also included the Business Officer group. (This is not pertinent to the use case, but was included here to demonstrate that groups can be assigned to groups)

Roles:

Two roles are defined in this scenario: Payroll Clerk, and payroll supervisor.
The roles, and the relevant permissions and responsibilities are shown here.

Payroll Clerk

- Type: Departmental
- Permissions:
    - Can View Payroll: Non-Exempt
- Responsibilities:
    - Approve Document: Timesheet

Payroll Supervisor

- Type: Departmental
- Permissions:
    - CanViewPayroll: All
    - MakeOrganization Group Changes
- Responsibilities:
    - FYI Document: Timesheet

Role Assignments:
In this example, the groups are assigned to the roles.

Namespace	Role Name	Type	Member ID	Name	Active From	Active To
Staff	Payroll Clerk	Group	Fin. Admin	n/a	01/01/2000	
Staff	PayrollSupervisor	Group	BusinessOfficer	n/a	01/01/2000	

Permissions / Responsibilities

Permissions and Responsibilities use templates to define the related attributes.

Approve Document Responsibility
  ApproveTemplate
    Type: Departmental
    Qualifiers:
      Document Type: Timesheet
      Route Status: Enroute

FYI Document Responsibility
  FYI Template
    Type: Departmental
    Qualifiers:
      Document Type: Timesheet
      Route Status: Approved&

CanViewPayroll:Non-Exempt Permission
  CanViewPayroll Template
    Type: Departmental
    Qualifiers: Employee Exempt Status: Non-Exempt

CanViewPayroll:All Permission
  CanViewPayroll Template
    Type: Departmental
    Qualifiers: Employee Exempt Status: Exempt, Non-Exempt

Use Case Action:
To replace Gina with Marcus, the department chair:

- Modifies Gina's Group Assignment, by setting the "Active To Date" with her end date.
- Adds Marcus to the FinanceAdminAssistants group with his start date as the "Active From" Date

Namespace	Groupname	Type	Member ID	Name	Active From	Active To Date
Staff	Finance Admin Assistants	Principal	100	Gina	6/30/1998	12/31/2009
Staff	FinanceAdmin Assistants	Principal	101	Marcus	01/01/2010	

Alternate Implementations
This model could have been created in a number of ways.
For example, it is not necessary to use groups at all, Gina and Marcus could have been assigned directly to their roles, instead of implicitly through their group assignments. If this were the case, it would be the role assignments that would be added/changed instead of the group assignments.

Dorm Access for Residential Advisors

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.

A possible Kuali Rice solution:

Permissions -- This scenario involves a single type of permission.
OpenDoor
KIM Type: Building Access
Attributes:
- Building \ Quad Name
- From Time
- To Time

KIM Type: Building Access
A new KIM Type "Building Access", specifies the attributes used to qualify permission instances related to building access. This KIM Type is a configuration item that is loaded into the Rice database.
A small amount of client code would be necessary to perform the permission matching logic.

Suppose we have the following Permission Instances.

Perm Name	Building	Time From	Time To	Description	PermI D
Open Door	Asia Hall	00:00:00	23:59: 59	Asia Hall 24/7 Access	401
Open Door	Africa Hall	00:00:00	23:59: 59	Africa Hall 24/7 Access	402
Open Door	Europe Hall	00:00:00	23:59: 59	Europe Hall 24/7Access	403
Open Door	America Hall	00:00:00	23:59: 59	America Hall 24/7 Access	404
Open Door	Australia Hall	00:00:00	23:59: 59	Australia Hall 24/7 Access	405
Open Door	Muir A	00:00:00	23:59: 59	Muir A 24/7 Access	406
Open Door	Muir B	00:00:00	23:59: 59	Muir B 24/7 Access	408
Open Door	--	08:00:00	22:00: 00	Dorm Daytime Access	410

This example defines the permissions for 2 Quads, one with 5 dorms, one with 2 dorms.

Roles
Three types of Roles defined in this scenario. Student, Resident, and ResidentAdvisor

Student
Permissions:
All Dorms Daytime Access

Resident
Role Attribute: Building \ Quad
Permissions:
Open Door: Building ID, Time of Day

Resident Advisor
Role Attribute: Building \ Quad
Permissions:
Open Door: Building ID, Time of Day

Instances of the Roles:

Role	Building / Quad Attribute	Permissions	Role Description
Resident	Asia Hall	Asia Hall 24/7 Access	Asia Hall Resident
Resident	Africa Hall	Africa Hall 24/7 Access	Africa Hall Resident

Resident Advisor	North Quad	Asia Hall 24/7 Access Africa Hall 24/7 Access Europe Hall 24/7 Access America Hall 24/7 Access Australia Hall 24/7 Access	North Quad RA
Resident	Muir A	Muir A 24/7 Access	Muir A Resident
Resident	Muir B	Muir B 24/7 Access	Muir B Resident
Resident Advisor	South Quad	Muir A 24/7 Access Muir B 24/7 Access	South Quad RA
Student	n/a	Dorm Daytime Access	Active Student

Role Assignments
Suppose:
- John is the RA for the North Quad
- Richard is a Resident in America Hall
- Janis is a student that lives off campus

Person / Group	Role Description	From Date	To Date
John	North Quad RA	09/02 /2009	12/31 /2009
Richard	America Hall Resident	09/02 /2009	12/31 /2009
Janis	Student	01/01 /2007	06/15 /2010

Note: John may also have Student, and Resident role assignments not shown here. And Richard may also have a student assignment not shown here.

Use Case Actions:
Assign Richard as a North Quad Resident Advisor for the time period during John's leave of absence
Change John's role assignment dates s to reflect the leave of absence.
For this example, assume the leave of absence is from Nov 15th until the end of the semester

The updated Role Assignments would be as follows:

Person / Group	Role Description	From Date	To Date
John	North Quad RA	09/02 /2009	11/14/2009
Richard	America Hall Resident	09/02 /2009	12/31 /2009
Richard	North Quad RA	11/15/2009	12/31/2009

Card System / KIM Logic Flow
Unicard system client invokes the KIMPermissionService.isAuthorized() method with the following parameters:
Principal ID: the ID of the person who's card was swiped.
Namespace: CampusSecurity
Permission Name - OpenDoor
Permission Details: Building \ Quad Name Time of Day

isAuthorized() then evaluates the permission details to determine if the principal is authorized.
First, get all of the Roles which have the permission that match the given details. Then the RoleService is invoked to determine if the principal belongs to any of these roles.

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).

Using KIM to grant access to the survey page:

Assume that the user has been authenticated via the Federated SSO system and has a unique ALA membership ID.

Group: ALA Members

Suppose we have a group "ALA Members" and that all of the affiliated librarians are assigned to this group.

Permissions:

Suppose we have created a permission template, "Access Page", to handle access to the various pages of the website. Permissions of this type take the page name as a quailifying attribute.
And that an instance of this permission, "Access Survey Page", has been created in KIM to grant access to the survey page.

Roles:

Suppose we have created the Role ALA Website User which contains the Access Survey Page permission (among others).

ALA Website User

- Type: Default
- Permissions:
  - Access Survey Page

Role Assignments: In this example, the group "ALA Members" has been assigned to the "ALA Website User" Role.

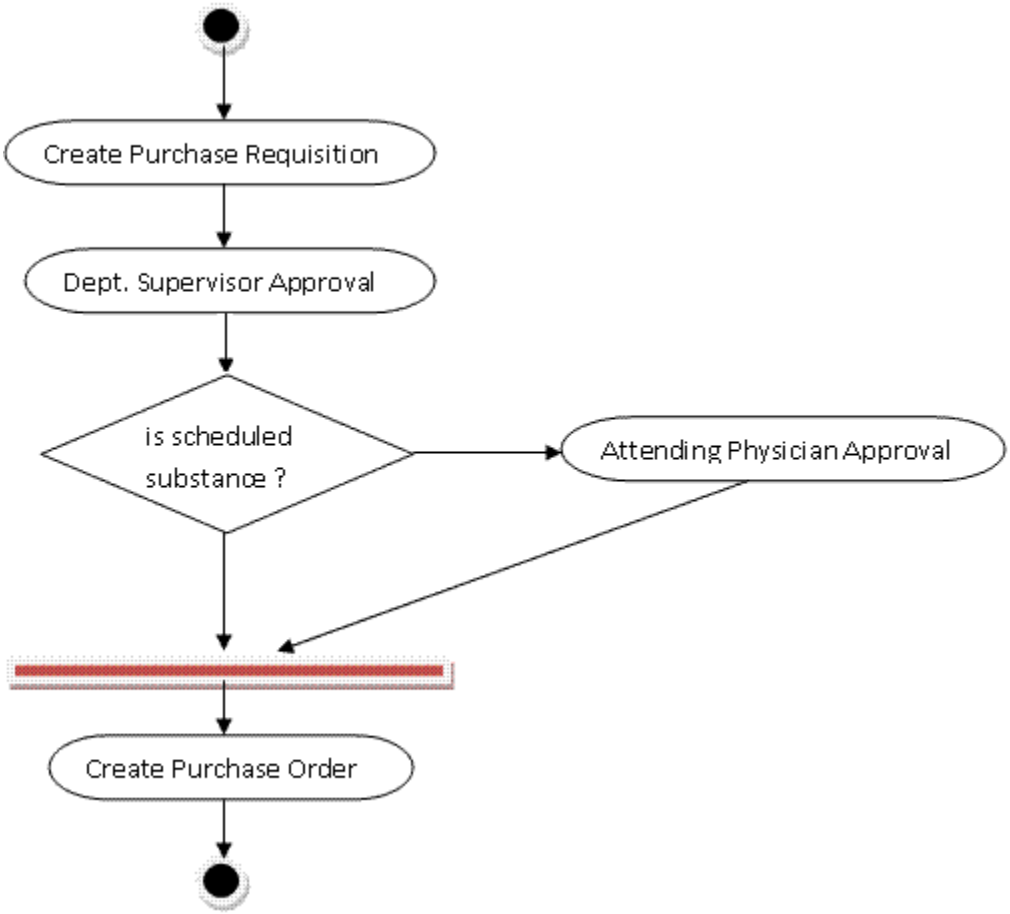
The code handling the page requests could then have a pre-processing step which invokes the KIM identityManagementService.isAuthorized() method. Passing in the users ID, and the page name as parameters.

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.

*A possible Kuali Rice solution:*This use case could be achieved within Kuali Rice by using a combination of the KEW workflow module and the KIM identity management module. Suppose a Pharmacy Purchase Requisition Workflow document has been defined.

The route path of the document has been defined as:



- Approve Document: Pharmacy Purchase Requisition

Attending Physician

KIM Types:

The KIM type identifies the set of qualifier attributes (fields). These qualifiers are used to separate different instances of types of group. In this case, each of the above groups has a KIM type of "Departmental". DepartmentCode This separates these groups by department. For example: Oncology Head Nurses from Maternity Head Nurses

Roles:

Three roles are defined in this scenario: Attending Physician, Head Nurse, Nurse

Nurse

- Type: Departmental
- Permissions:
  - Can Create Document: Pharmacy Purchase Requisition

Head Nurse

- Type: Departmental
- Permissions: - All nurse permissions plus others
- Responsibilities

- Type: Departmental
- Permissions:
    - Can Create Document: Pharmacy Purchase Requisition
    - Can Create Document: Prescription
    - Can Blanket Approve Pharmacy Purchase Requisition
    - Can Blanket Approve Prescription
- Responsibilities
    - Approve Document: Phamarcy Purchase Requisition

Permissions / Responsibilities

Permissions and Responsibilities use templates to define the related attributes.

Approve Document

- Attributes:
    - Document Type: Pharmacy Purchase Requisition
    - Route Status: Enroute

Can Create Document

- Attributes:
    - Document Type: Pharmacy Purchase Requisition

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.

Use Case Assumptions:

a) Suppose the Active Directory system has been integrated to use the Rice KIM module to manage access authorizations.??

OR

b) Or the Active Directory is also integrated with KIM to implement portions of the KIM's IdentityManagement Service. Specifically, the underlying KIM services: IdentityService and IdentityUpdateService (and perhaps PersonService, and AuthenticationService)

OR

c) we have some other application a layer above the Active Directory that manages access.

KIM Types:

In this case, the above group has a KIM type of "College&Dept" which defines two attributes

- College
- Department

Groups:

Suppose the group type IT Administrators has been defined and is qualified by College and Department.
And that there are several instances of this group type representing the various departments including

IT Administrators:Arts and Sciences:Chemistry
IT Administrators:Arts and Sciences:null

Group Assignments at the beginning of this scenario could be as follows:

Namespace	Groupname	Type	Member ID	Name	Active From	Active To Date
Staff	IT Administrators:Arts and Sciences:Chemistry	Principal	100	Bill	6/30/1998	
Staff	IT Administrators:Arts and Sciences:Chemistry	Principal	101	Betty	01/01/2009	
Staff	IT Administrators:Arts and Sciences:Chemistry	Principal	102	Ben	04/01/1990	

Staff	IT Administrators:Arts and Sciences:null	Principal	103	Patrick	10/10/2002	

Bill and his two co-workers are assigned to the IT Administrators:Arts and Sciences:Chemistry group.
Patrick is assigned to the IT Administrators:Arts and Sciences group.

Roles:

Suppose we have created the role WinPCandFileServerAdmin

WinPCandFileServerAdmin

- Type: College&Dept
- Permissions:
  - Update Home Directory
  - Update Home Drive

In this example, the group ITAdministrators is assigned to the role

Namespace	Role Name	Type	Member ID	Name	Active From	Active To
Staff	WinPCandFileServerAdmin	Group	IT Administrators	n/a	01/01/2000	

In this scenario, Bill has the ability to update the home directory and drive for users in his department, but not the msExchgHomeServerName.

Patrick has the ability to update the home directory and drive for all users in the college. Since his department attribute is null, he has access to all departments within the college.

When Bill returns from Switzerland, he is simply removed from the IT Administrators:Arts and Sciences:Chemistry group by updating the ActiveTo field in the group assignment.

Namespace	Groupname	Type	Member ID	Name	Active From	Active To Date
Staff	IT Administrators:Arts and Sciences:Chemistry	Principal	100	Bill	6/30/1998	01/04/2010