MACE-paccman comparative taxonomy

Comparative Taxonomy

Comments and feedback are welcome and encouraged. Authenticated users may post comments, or you may send e-mail to <mace-paccman-contact AT internet2 DOT edu>. Instructions for obtaining editing access can be found at http://middleware.internet2.edu/docs/internet2-spaces-instructions-200703.html.

Purpose:

During the EDUCAUSE and Internet2 Advanced CAMP in June 2009, participants suggested that MACE-paccman create a comparative taxonomy that would explore the differences, as well the commonality, between several systems that have importance or relevance to the CAMP attendees and the MACE-paccman community.

The following were suggested as projects to include in this comparison: Grouper, perMIT, Sakai 2, KIM, Kulai Student, IMS, the Spring Security framework (formerly known as ACEGI), Moodle, Sun's Identity Manager, Oracle Identity Manager, XACML.

Proposed Model:

The proposed model is to start with the terms included in the paccman glossary and have someone familar with each project fill in a section of the document that compares and contrast the systems usage of the term with the base glossary definition and the other projects or products.

Access Control	**The act of allowing access to facilities, programs, resources or services to authorized persons (or other valid subjects), and denying unauthorized access. Access Control requires that rules or policies be in place, that privileges be defined, so that they can be enforced.**
Grouper	
perMIT	The perMIT project's view is aligned with the current definition.
Sakai 2	
KIM	
Kuali Student	
IMS	A security technology that selectively permits or prohibits certain types of data access based on the identity of the accessing entity and the data object being accessed.[Note 1]
Spring Security	Spring security's usage of "access control" is well aligned with the current definition.
Moodle	
Sun IDM	
Oracle IDM	Oracle IdM uses the term "access" instead of "access control", but the definition is otherwise well aligned.

Access Management	**That part of Identity Management comprising the processes and tools used to associate privileges with subjects in accord with the wishes of Authorities.**
Grouper	
perMIT	
Sakai 2	
KIM	The KIM use of this term is well aligned with this definition.
Kuali Student	
IMS	*Access Management Service:* The application of data about users, user profiles and services to access control systems so that authenticated users have access to those system, functions and resources that they are authorized to use. Typically Access Management Systems also seek to support single sign on, where the user is challenged for a single name and password and has access to more than one system or resource.[Note 1]
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	Oracle IdM uses the phrase "access rights management" to denote those processes by which access is granted or revoked.

Assertion	**A declaration or claim. Typically, when the term *assertion* is used in conjection with privilege management it tends to connote a claim formatted with a particular formal syntax. For example the document or speaker may be talking about a claim formatted as an assertion conformant to the SAML specification.**
Grouper	
perMIT	perMIT does not currently create any SAML assertions. Nor does is currently consume and SAML assertions. One request has been made for the system to accept SAML assertions and have this trigger a rule evaluation that would create an ASPEC, if applicable, on the fly.
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	OIM doesn't currently employ any claims-based or assertion-based facilities. OAM (Oracle Access Manager)
XACML	A specific characteristic of a subject, resource, action or environment in which the access request is made. Attributes could include a user's name, workstation identity, security clearance, the file to which access is desired and the time of day.

ASPEC	
Grouper	
perMIT	We believe this term is unique to perMIT. We created the term so that we would not cause any confusion with common, overloaded terms, or establish a colloquialism. An ASPEC refers to a perMIT triple consisting of a subject + function + qualifier.
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	

Authentication	**The process of confirming the identity of a principal. Since computer identification cannot be absolute (e.g., passwords can be stolen), authentication relies on a related concept of *level of trust*, in which an institution relies on good identity management practice (so that the institution believes they have correctly identified an individual) and secure mechanisms for sharing identity. This is sometimes referred to as *AuthN* (authentication), in contrast to *AuthZ* (authorization).**
Grouper	
perMIT	
Sakai 2	
KIM	The KIM definition is aligned with this definition. In the current KIM technical guide, authentication is defined as the act of logging into the system.
Kuali Student	
IMS	Verifying a user's claimed identity.[Note 1]
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	

Authority	**1) A broad term than can cover most aspects of creating policies and rules governing who has rights and privileges for an organization. It includes the ability to control the dissemination of those rights, as well as an organization's responsibilities to enforce those rights. This is sometimes referred to as AuthZ (authorization), in contrast to AuthN (authentication).** **2) It can also refer to a person or policy or rule that confers privileges to subjects, either directly by use of an access management system, or indirectly.** **3) It can also be used more specifically in a singular authorization situation to say whether a principal has "authority" to take an action. In this sense, authority and privilege can be used interchangeably.**
Grouper	
perMIT	see also: primary authorizer, principal investigator, and grantor
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	Sun IDM uses the term "capability" to describe #3
Oracle IDM	

Authorization	**The process of deciding if a subject (person, program, device, group, role, etc.) is allowed to have access to or take an action against a resource. Authorization relies on a trusted identity (*authentication*) and the ability to test the privileges held by the subject against the policies or rules governing that resource to determine if an action is permitted for a subject.**
Grouper	
perMIT	
Sakai 2	
KIM	The permission for a principal to perform actions in the system.
Kuali Student	
IMS	The permission to perform certain operations or use certain methods or services.[Note 1]
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	

Claim	**A declaration, or assertion, made by an entity. Hopefully the entity is a reliable third party. Examples of claims include names, affiliations, group membership, or capabilities.**
Grouper	
perMIT	
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	
Kim Cameron	an assertion made by one subject about itself or another subject that a relying party considers to be "in doubt" until it passes "Claims Approval"

Delegation	**The process used, or task performed, by a grantor to assign privileges to other subjects within the limits of its authority. A subject with delegated privileges does not have to perform any type of impersonation in order to exercise the privileges.**
Grouper	
perMIT	
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	The process of temporarily assigning future work items to one or more other users for a specified period of time.
Oracle IDM	Roughly speaking, in OIM, granting or revoking access is referred to as "provisioning" or "deprovisioning", and he process used by a grantor to assign or revoke resource access for a subject is reerred to as "direct provisioning" (as opposed to access granted or revoked automatically based on rules). OIM reserves the term "delegation" for the process of authorizing an OIM user to perform provisioning or deprovisioning.

Eligibility	**A concept closely related to authorization in that it can use the same mechanisms of authentication, policies, rules, and role evaluation. The differences are semantic - one is "eligible for something" as opposed to "authorized to do something" - so each is appropriate to use to describe different use cases. For instance, "all students are eligible for an email account", vs "students in this class are authorized to download course materials".** **Eligibility is more akin to a "right", in legal terms, than a "privilege", but the technical differences in how they are accomplished in an online environment are generally negligible.** **The term has sometimes been used in circumstances in which subjects must take a specific step in order to receive an authorization.**
Grouper	
perMIT	perMIT does not support the management of eligibility. The only portion of perMIT that might touch on eligibility is the implied *authorizations subsystem* , in that data that expresses an eligibility might be evaluted and corresponding ASPECs might be created as a result.
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	The concept of "eligibility" arises in OIM in reference to the application of rules to grant or revoke access. The term isn't really used much in the documentation, but the concept surfaces in multiple forms.

Entitlement	**Often used the same as Privilege, entitlement carries the feeling of something owed or of a right granted. We make limited use of the word here. An authority-related eduPerson attribute - eduPersonEntitlement - uses this term specifically as an attribute that conveys ownership of the named right or privilege, a token that can be used directly or in a rules evaluation in determining authorization.** **It's noteworthy that privileges with qualifications, limits, scope, attributes, conditions, or prerequisites aren't called entitlements. It seems to be used only for simple, non-parameterized expressions.**
Grouper	
perMIT	perMIT does not attempt to manage entitlements. By their nature perMIT ASPECs always include a scope (aka qualifier), although in some cases the scope may be NULL.
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	

Entity	**A collection of identifiers and attributes managed by an Identity Management System representing any real-world actor, such as a person, process, system, etc. This is very similar to one definition of Subject below, with the possible distinction that a Subject can represent groups and roles in addition to real-world actors.**
Grouper	In the Grouper UI, the term Entity is used instead of Subject, since it is more natural for non technical people
perMIT	
Sakai 2	
KIM	The KIM definition is well aligned with this definition. KIM definition: A record responsible for housing identity information for a given Person, Process, System, etc.
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	

Grantor	**A principal authorized to delegate some portion of its own authority and that has exercised that privilege.**
Grouper	
perMIT	
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	

Group	**A collection of subjects, which can include subjects representing other groups.**
Grouper	
perMIT	
Sakai 2	
KIM	The KIM definition is well aligned with this definition. A group is a collection of principals. You can create a group using both direct principal assignment and nested group membership. All groups are uniquely identified by a namespace code plus a name. A principal or group is a "member" of a group if it is either directly assigned to the group or indirectly assigned (through a nested group membership). A principal or group is a "direct" member of another group only if it is directly assigned as a member of the group, and not through a nested group assignment.
Kuali Student	
IMS	*Group Management Service:* Group management services can include data from class creation and class scheduling, and the ongoing maintenance of that data. A source system creates and maintains group information, which needs to be shared with other systems that are involved with group management functions. The flow of group management information is not necessarily one way; some data may be updated by a target system and passed back to the source system.[Note 1]
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	

Identity Management	**Identity management is often used broadly to encompass not only activities to correctly identify and maintain attributes about subjects, but also the manifestations of that knowledge through infrastructure supplying access and security services - single sign-on, account/service provisioning, authentication and authorization. Here we focus on a narrower definition, principally the need to identify persons as one individual despite multiple associations and roles, proper identification of other entities and agents (organizations, applications, groups, services, resources, etc), and the management of that information over time and across the enterprise. Sometimes the term "Identity and Access Management" is used to be explicitly inclusive of access management within this practice. When the number of subjects that need to be given identifiers for use in Identity and Access Management systems is very large, the ability to name things may itself be controlled by access management. This requires an underlying identity management practice for namespaces.**
Grouper	
perMIT	
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	

Member	
Grouper	A member in Grouper is a subject used in Grouper (e.g. a member of a group). Each subject has a member record in the Grouper system.
perMIT	
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	

Membership	
Grouper	A membership is an assignment of a group to a member/subject, and a list. A group can have multiple lists (e.g. a class group could have a students list and a teachingAssistants list. A list can also be referred to as a field.
perMIT	
Sakai 2	Several important types of group (site memberships; course sections; integration with a group provider such as SIS or LDAP) include *role* as an aspect of membership. E.g., a member of an official course offering may play the role of "Instructor of Record" or "Enrolled Student."
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	

Namespace	**A domain in which an identifier is unique in representing a single object.**
Grouper	Grouper has stems (aka folders) in which objects can be assigned. A group and a stem can have the same name in the same stem.
perMIT	
Sakai 2	In Sakai 2, the Site is the main organizational unit. Instances of plug-in tools are added to a site. Groups and sections are managed as subgroups of the site membership. In Sakai 3, workspaces and groups will be managed and associated more flexibly.
KIM	The KIM definition of namespace is aligned with this definition.

Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	The closest term to this is Schema Map in the Sun IDM
Oracle IDM	

Permission	**A closely related term to *access control*, a permission is the control specifically related to a resource and an action - a subject must have permission to take that action. Note - paccman is deprecating this term and suggest that privilege be used consistently.**
Grouper	A permission in Grouper refers to external permissions that an external system might be managing centrally with grouper. This is a type of attribute on a Role or a Role/Subject tuple (how individual permissions are assigned, not Role-wide).
perMIT	
Sakai 2	In Sakai 2, "permissions" are string keys registered for external management and used by an application or service to distinguish user access rights: a plug-in calls the framework to find out whether the current user has the given permission in the current context. The framework generally decides this based on mappings of site membership role to permissions. Not all access decisions need be exposed for external management. Some permissions might be shared by multiple components. Coarsely-grained permissions based on application workflow sometimes overlap conceptually with roles.
KIM	KIM use of this term is similar. Defined as the fine grained actions that can be mapped to functionality within a given system.
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	user entitlementIn Identity Manager, an auditable access privilege granted to a user on a resource or system that enforces access restrictions.
Oracle IDM	

policy	**A policy is used to describe general access control requirements. There are many existing proprietary and application-specific languages for creating policies, but XACML has several points in its favor: it's standard, it's generic, it's distributed, it's powerful.** **A XACML policy has at least one, and possibly more rules. A policy may be written to have a single effect, meaning that each policy has a single rule that either permits or denies access. This style of policy writing results in many individual policies, but each policy is atomic and uncomplicated. An alternative is to have fewer policies, each with multiple rules within.** **A XACML policy contains one or more RULEs, which may contain a TARGET and a CONDITION. A TARGET consists of a SUBJECT, an ACTION, a RESOURCE, and optionally an ENVIRONMENT. RULEs can be composited.**
Grouper	
perMIT	A perMIT ASPEC can be easily translated into a single effect XACML policy, and vice versa. If more complicated policies are desired, within perMIT, this would be done when creating the rules for implied authorizations. The more complicated rules will always end up being expanded into the simple ASPEC model within the perMIT database.
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	Establishes limitations for Identity Manager accounts. Identity Manager policies establish user, password, and authentication options, and are tied to organizations or users. Resource password and account ID policies set rules, allowed words, and attribute values, and are tied to individual resources.
Oracle IDM	

Principal	**A subject whose identity can be authenticated.**

Grouper	
perMIT	
Sakai 2	
KIM	KIM definition is very similar. Uses the term entity instead of subject.
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	The equivalent word is account
Oracle IDM	

Privileges	**Etymologically speaking, a privilege is a "personal law", making privileges a set of personal rights. Privileges amount to the sum of what a subject may do, as granted to them or inherited. In the context of a Privilege management system, Privilege is used to describe the combination of a subject or group, their current allowable actions, and any qualifications or scoping limitations that shall be imposed on those allowable actions.**
Grouper	A privilege in Grouper refers to privileges on Grouper objects. e.g. someone can UPDATE a group (change the membership list), or CREATE in a stem/folder (they can create objects there. Since Grouper has internal privileges, and can act as a privilege management system, the internal privileges are privileges, and the external ones are permissions.
perMIT	Etymologically speaking, a privilege is a "personal law", making privileges a set of personal rights. Privileges amount to the sum of what a subject may do, as granted to them or inherited. Privilege is used to describe the combination of a subject or group, their current allowable actions, and any qualifications or scoping limitations that shall be imposed on those allowable actions. *Groups or roles do not have privileges, but instead provide a mechanism to confer privileges to all members of a group or role as individual principals.*
Sakai 2	
KIM	KIM currently uses the term permission.
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	user entitlementIn Identity Manager, an auditable access privilege granted to a user on a resource or system that enforces access restrictions.
Oracle IDM	

Provisioning	**The process of managing attributes and accounts within the scope of a defined business process or interaction. Provisioning an account or service may involve the creation, modification, deletion, suspension, or restoration of a defined set of accounts or attributes.**
Grouper	Grouper has the "Grouper loader" which keeps groups in sync with external systems (currently via SQL). It also has a change log and notifications, and ldappc (ldap provisioning connector) to export data out of grouper.
perMIT	
Sakai 2	Sakai uses a user directory provider and a group provider as integration points with external authentication, person profile, personnel, and course systems.
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	This matches the Sun IDM
Oracle IDM	

Resource	**Resource and Target are often used synonymously when discussing privilege management colloquially. As with Target, the term is context dependent when used informally. At times, Resource is another close synonym of Qualifier and Scope. However, people tend to use this term when speaking about more "tangible" scopes such as "Oxford English Dictionary Online" or "Ethnic Newswatch". There are other qualifiers and scopes that people don't typically think of as a resource, for example "the category of HR", "NULL", and depending how closely you work with the financial system, cost objects and account numbers.** **See Qualifier**
Grouper	
perMIT	see Qualifier
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	
XACML	In XACML, the resource is the *"thing"* which is being managed.

Responsibility	
Grouper	
perMIT	perMIT does not distinguish between a Function and a Responsibility. Since functions are defined in bussiness terms, we don't see this as a problem. For example within our Payroll category we have a function named EDACCA CERTIFIER-PERCENT ONLY. This means an individual with direct knowledge of the work performed who is authorized to certify the DACCA without maintaining paper back up, with access by percentage and not by dollar amount.The qualifiers are used to control this by profit center, a profit center or cost object supervisor, or at a cost object. The privilege management system does not care if the person simply has the privilege, or if the person actively uses the privilege. On the other hand, the business processes and people responsible for payroll certainly do expect that people that have this privilege are performing the necessary actions, in accordance with all of the applicable policies.
Sakai 2	
KIM	A responsibility is an action that a principal assigned to a role is expected to perform. Similar to a permission except that the principal not only has the ability to perform the action, but is expected to perform the action. This is used for defining workflow actions (such as approve, acknowledge, FYI) for which the principal is responsible. Responsibilities form the basis of the workflow engine routing process.Responsibilities are always granted to a role, never assigned directly to a principal or group. Furthermore, similar to permissions, a role has a responsibility template. The responsibility template specifies what additional responsibility details need to be defined when the responsibility is created.
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	The Sun IDM has the notion of an approval chain which indicates the individuals in a workflow that need to approve a role assignment
Oracle IDM	

Role	**A collection of *privileges* usually relating to a task, responsibility, or qualification associated with an enterprise. Collections may be comprised of any combination of implicitly and/or explicitly defined privileges. Roles within an enterprise typically have overlapping privileges. Role based access control systems often include features to establish role hierarchies, where a given role can include all of the privileges of another role. Roles can generally be associated with subjects (person, program, device, group, etc.)**
Grouper	A Role in Grouper is what links subjects (including Groups), to permissions. It is similar in structure to a group (has an internal name, friendly name, description, namespace, members). A Role in Grouper can be in a directed graph of Role inheritance. So a Role can inherit permissions from other Roles.
perMIT	Roles are associated with a subject, but a subject cannot be a group within perMIT.There are two mechanisms to create a collection of privileges within perMIT. One method is to use function inheritance. When using function inheritance, when one ASPEC is created, multiple related ASPECs will be created. However, the qualifier will be identical for all of the generated ASPECs. This means that you cannot have parent-child function relationships that require different qualifier types. If a role requires the creation of multiple ASPECs that use distinct qualifier values and/or qualifier types, the "implied authorization" subsystem may be used. The subsystem provides the ability to create rules which will create multiple ASPECs and the generated ASPECs may use different qualifier data types. ASPECs may even be created in multiple categories.

Sakai 2	A role indicates a person's tasks, responsibilities, qualifications, or expectations in some context. It may be associated with a collection of software privileges or permissions. It may determine an application's UX (e.g., the blog presents different workflows to the the owner and the commenter). It may be used to map between disparate contexts. E.g., externally-managed course management groups and roles (official classes and sections; "Instructor", "Enrolled Student", "Teaching Assistant") can feed Sakai 2 site memberships and roles. Sakai 3 also intends to support social networking contexts which use "relationship to a person" in much the same way as "role in a group."
KIM	Roles aggregate permissions and responsibilities. Roles are not scoped to namespace therefore, Roles can provide authorization privileges across namespace Roles have a membership consisting of principals, groups, and/or other roles. As a member of a role, the associated principal has all permissions and responsibilities that have been granted to that role. Roles can also have arbitrary data associated with them (i.e. Role Attributeshttps://test.kuali.org/confluence/display/KULRICE/KIM+Glossary#KIMGlossary-roleattribute) for scoping or classification purposes which can help to qualify authorization checks at a very limited fashion.
Kuali Student	
IMS	A specification of the type of participant in a unit of learning. There are two basic role types-Learner and Staff, which can be sub-typed to allow learners to play different roles in different learning activities (e.g., task-based, role-play, simulations). Similarly support staff can be sub-typed and given more specialized roles, such as Tutor, Teaching Assistant, Mentor, etc. Roles thus lay the basis for multi-user models of learning.[Note 1]
Spring Security	
Moodle	
Sun IDM	A role is an Identity Manager object that allows resource access rights to be grouped and efficiently assigned to users. Roles are organized into four role types: Business Roles, IT Roles, Application Roles, and Assets. IT Roles, Applications, and Assets organize resource entitlements into groups. These three groups are then assigned to Business Roles so that users can access the resources they need to do their jobs. However
Oracle IDM	

Rule	**A prescribed evaluation of data which is used to confer a privilege, or privileges, to a subject or a collection of subjects.**
Grouper	
perMIT	
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	Object in the Identity Manager repository that contains a function written in XPRESS, XML Object, or JavaScript languages. Rules provide a mechanism for storing frequently used logic or static variables for reuse within forms, workflows, and roles. Similar to the about definition
Oracle IDM	

Subject	**An entity whose identifiers and attributes are managed by an Identity and Access Management practice.**
Grouper	Same as definition above. Grouper uses the Internet2 Subject API so that several subject sources can be configured. Grouper implements some subjects sources for internal subjects (e.g. groups as subjects, GrouperSystem (all powerful user), and GrouperAll (if making a privilege public, assign GrouperAll to it)
perMIT	The noun in an ASPEC. A person, program, device, or other relevant entity which can authenticate to a system, and to which an authorization may apply. (Note well: A subject is never a *group*, since a group does not authenticate.)
Sakai 2	
KIM	KIM uses the term principal.
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	

XACML	The person or computer making a request.	
Kim Cameron	The consumer of a digital service (a digital representation of a natural or juristic person, persona, group, organization, software service or device) described through claims.	

Target	**The term "Target" should be deprecated. Target is a matter of perspective and context. When people are discussing privilege and access control informally, a target is often the same as a Resource. However, at other times, the focus is on the Subject. In yet different contexts the target is actually the set of people that have a specific verb and scope applied to them, as in the "target group".**
Grouper	
perMIT	
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	
XACML	A Target is basically a set of simplified conditions for the Subject, Resource and Action that must be met for a PolicySet, Policy or Rule to apply to a given request.

Verb	**See *Function***
Grouper	
perMIT	
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	
Oracle IDM	
XACML	
Kim Cameron	

Workflow	**Workflow is concerned with the automation of procedures where documents, information or tasks are passed between participants according to a defined set of rules to achieve, or contribute to the authority assigning privileges.**
Grouper	
perMIT	
Sakai 2	
KIM	
Kuali Student	
IMS	
Spring Security	
Moodle	
Sun IDM	

Oracle IDM	
XACML	
Kim Cameron	

Notes:

1. IMS definitions are taken from the IMS Abstract Framework Glossary, Version 1.0.