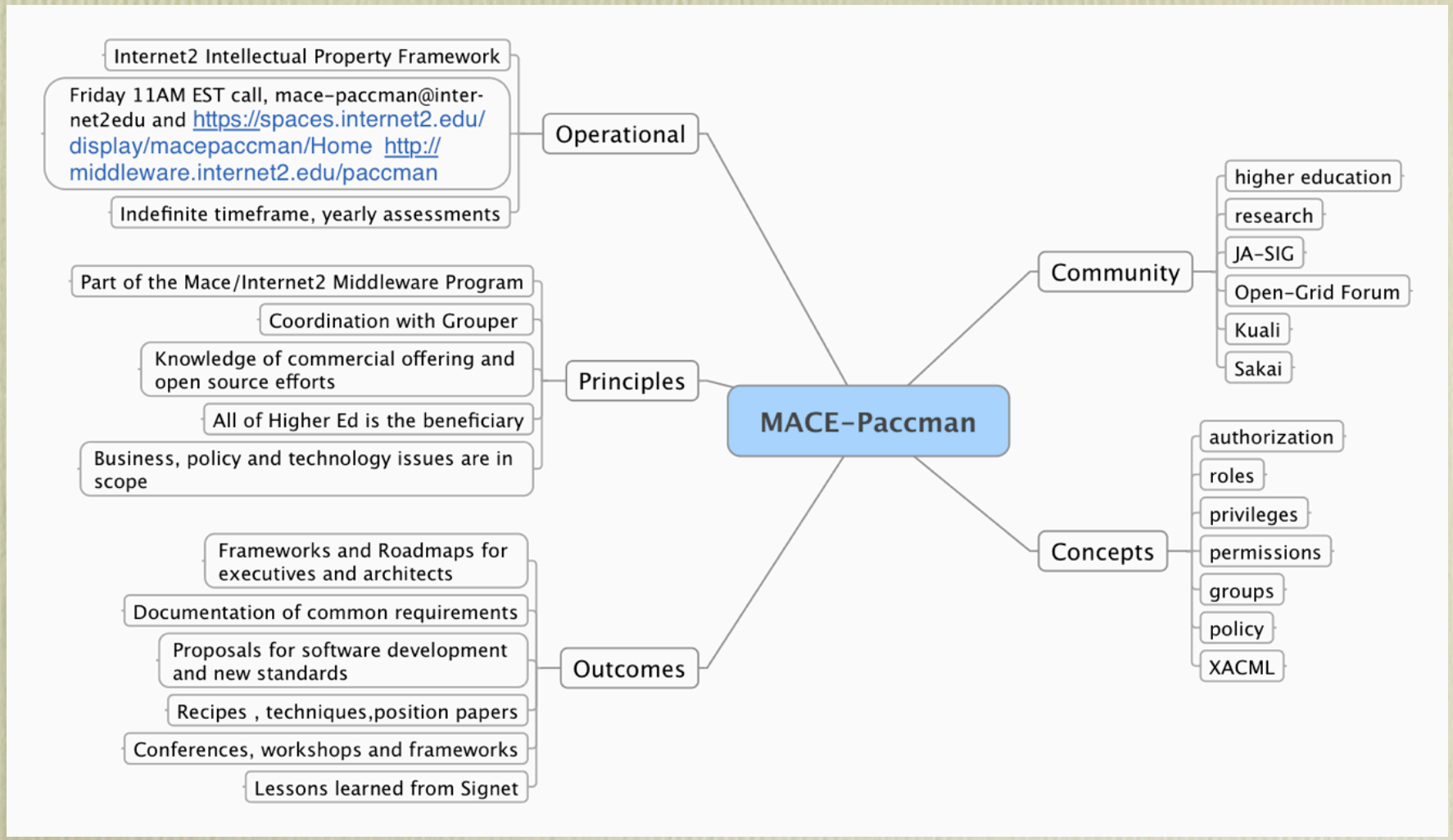
MACE-PAccMan Glossary and Comparative Taxonomy

ACAMP 2010

Rob Carter, Duke University

PAccMan Refresher



PAccMan Refresher

- Early, focus was on use cases -- defining the Privilege and Access Management problem space
  - https://spaces.internet2.edu/display/macepaccman/Use+Cases

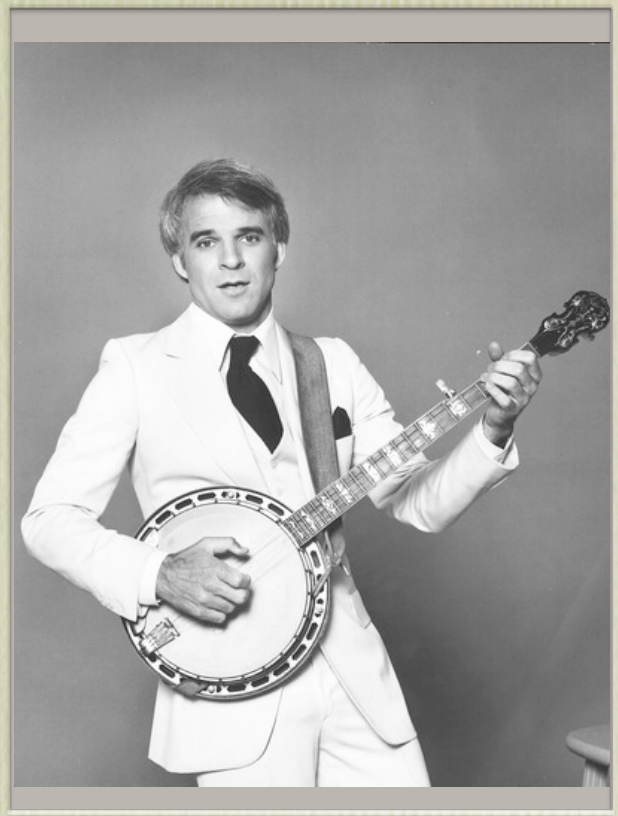
PAccMan Refresher

- More recently, focus has been on:
  - Comparison/Contrast of existing privilege and access management solutions (Grouper, perMIT, Oracle/Sun, KIM, etc.) and terminology
    - https://spaces.internet2.edu/display/macepaccman/Selected+Use+Cases
  - API considerations for Privilege/Access Management
    - https://spaces.internet2.edu/display/macepaccman/Permissions+API+suggestion+based+on+Grouper+permissions

Why Glossary: A not-quite allegory

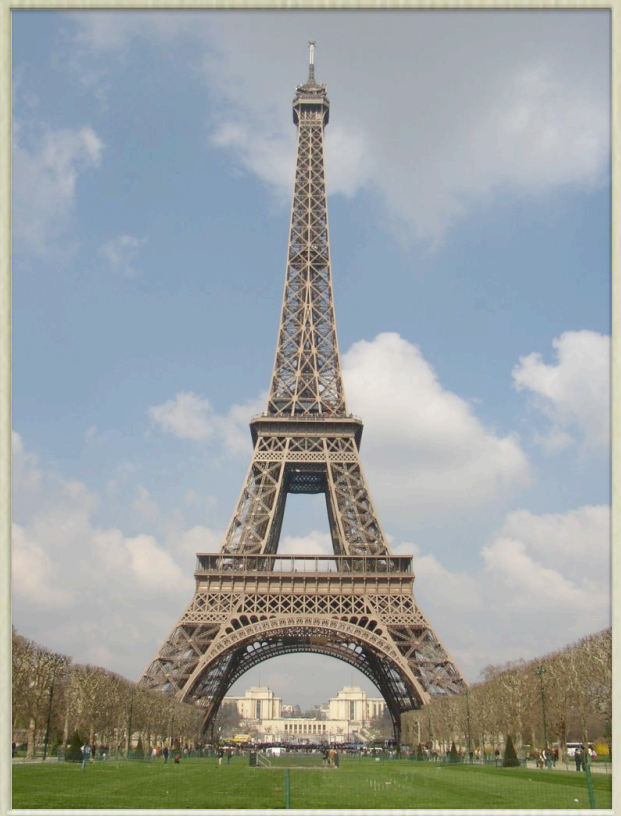
Glossary

Once upon a time, a very wise man...



Glossary

...traveled to a foreign country, and had a revelation...



Glossary

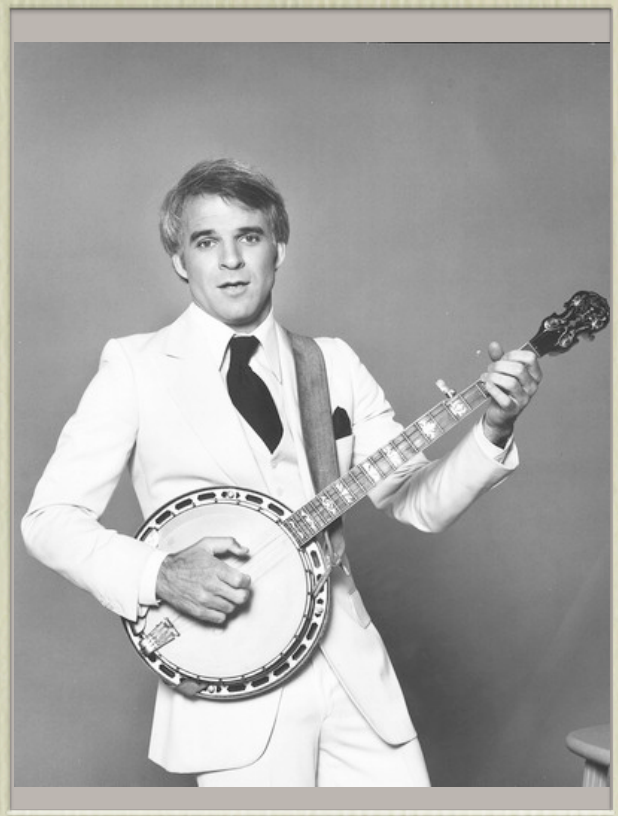
In France, “oeuf” means “egg”...

Glossary

...and “chapeau” means “hat”...

Glossary

"It's like those French have a different word for **everything!**"



Glossary

Realizing the wisdom of his words...

Glossary

Realizing the wisdom of his words…and the dangers of such confusion…

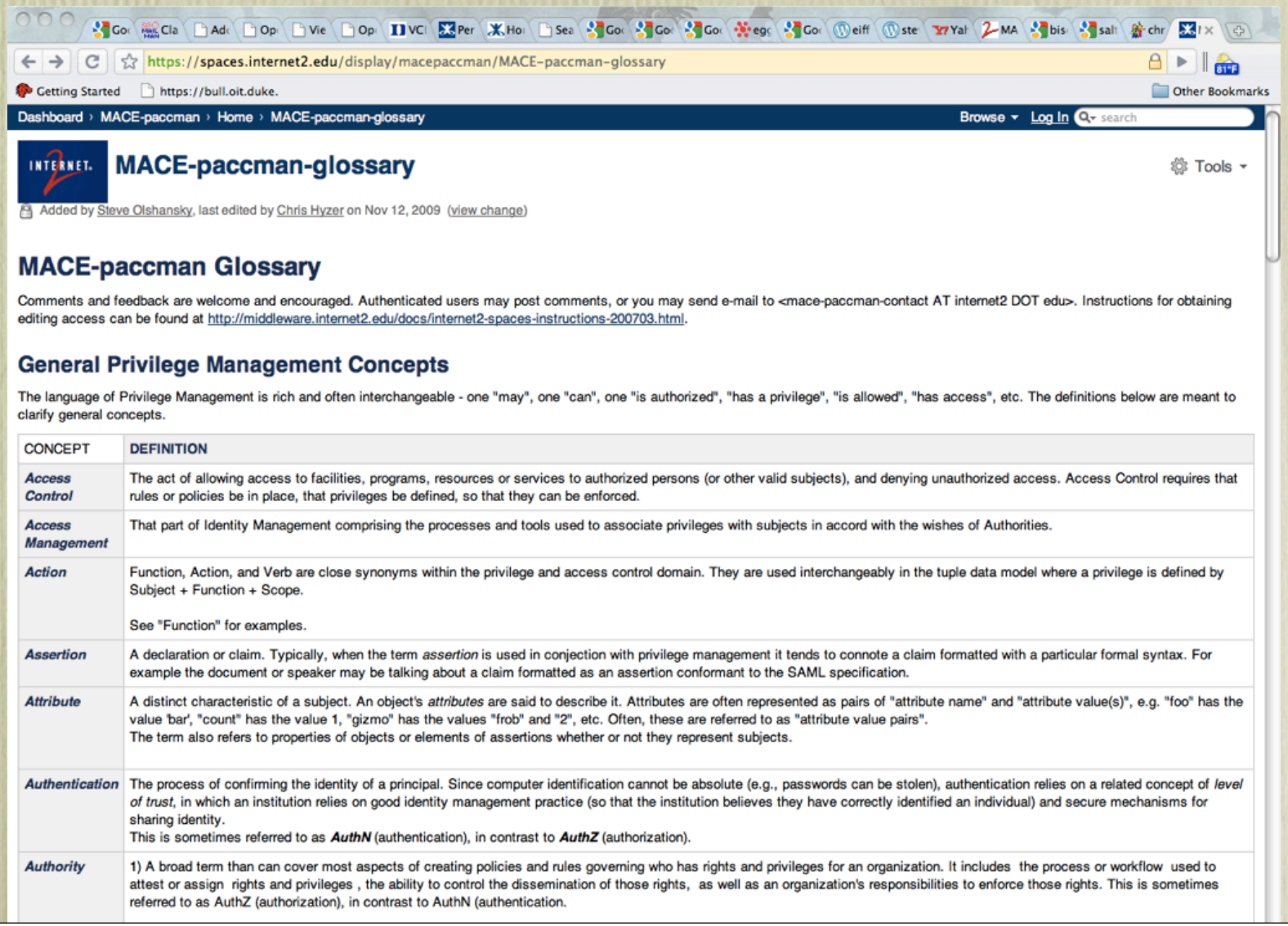
Glossary

- Discussed as an AI for the group during ACAMP 2009
- Work started before ACAMP, continued after...
- https://spaces.internet2.edu/display/macepaccman/MACE-paccman-glossary

Glossary

- Started as a way to normalize terminology during concalls, etc.
- Took on a life of its own for a while
  - Psycholinguistics -- the words we use shape the way we think
  - Led us to begin comparison/contrast of privilege/access management across industry

Glossary



https://spaces.internet2.edu/display/macepaccman/MACE-paccman-glossary

Getting Started https://bull.oit.duke. Other Bookmarks

Dashboard › MACE-paccman › Home › MACE-paccman-glossary Browse Log In search

MACE-paccman-glossary

Tools

Added by Steve Olshansky, last edited by Chris Hyzer on Nov 12, 2009 (view change)

MACE-paccman Glossary

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.

General Privilege Management Concepts

The language of Privilege Management is rich and often interchangeable - one "may", one "can", one "is authorized", "has a privilege", "is allowed", "has access", etc. The definitions below are meant to clarify general concepts.

CONCEPT	DEFINITION
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.
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.
Action	Function, Action, and Verb are close synonyms within the privilege and access control domain. They are used interchangeably in the tuple data model where a privilege is defined by Subject + Function + Scope. See "Function" for examples.
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.
Attribute	A distinct characteristic of a subject. An object's *attributes* are said to describe it. Attributes are often represented as pairs of "attribute name" and "attribute value(s)", e.g. "foo" has the value 'bar', "count" has the value 1, "gizmo" has the values "frob" and "2", etc. Often, these are referred to as "attribute value pairs". The term also refers to properties of objects or elements of assertions whether or not they represent subjects.
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).
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 process or workflow used to attest or assign rights and privileges , 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.

Comparative Taxonomy

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	

A quick example...

- **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. She logs into the hospital's online ordering system to submit a restocking request. 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 quick example...

- **Sun IDM Terminology** -- Nurse Wilson notices during a routine inventory review that the Oncology ward's drug cabinet is running low on a particular anti-emetic drug. She authenticates with an account to the resource “online ordering system” which has the entitlement “submit restocking request”. The anti-emetic is a scheduled substance, so she lacks the capability “approve restocking request” - policy requires that two other accounts engage in an approval workflow. 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 quick example...

- **KIM Terminology** -- Nurse Wilson notices during a routine inventory review that the Oncology ward's drug cabinet is running low on a particular anti-emetic drug. She logs into the hospital's online ordering system as a principal whose permission includes submitting restocking requests. The anti-emetic is a scheduled substance, so her request to the Pharmacy for restocking requires approval by principals whose roles include the responsibility for approving general requests from nurses and for authorizing release of scheduled substances . 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 quick example...

- Sun's IDM (RIP?) refers to authentication, accounts, resources, policies, workflows
- Kuali refers to logging in, principals, roles, responsibilities
- Here, the two may be less like French and English and more like English and American, but, if you've ever ordered crackers at a British pub...

FAL LA LA
FAL LA LA

A somewhat more involved example...

- **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.

A somewhat more involved example...

- **perMIT Approach** -- Gina, who's listed in a collection of perMIT ASPECs with qualifiers limiting their scope to the Chemistry department and its associated cost and payroll codes that enumerate the functions her job requires her to perform financial systems, vacates her position in the department to take a new position in the Office of the Comptroller. The department chair (who's listed in an ASPEC with the function "Financial Primary Authorizer" and the qualifier "Chemistry Department") chooses his executive assistant, Marcus, to take over as payroll clerk for the department. The department chair logs into perMIT and copies the ASPECs held by Gina to Marcus, assigning Marcus the same ASPECs Gina has had. perMIT later notifies the chair of Gina's official relocation and presents him with a list of her existing ASPECs. He deletes those already copied to Marcus, and reassigns others through the perMIT UI to other staff.

A somewhat more involved example...

- **Rice approach** -- Gina, an active member of an instance of the "Financial Assistants" KIM group with group type "Departmental" and DepartmentCode "Chemistry", which has been added to the role "Payroll Clerk", vacates her position in the department to take a new position in the Office of the Comptroller. The department chair, who is a member of the DeptChair group, which is in turn a member of the Business Officer group assigned to the role (among others) "Payroll Supervisor" chooses his executive assistant, Marcus, to take over as payroll clerk for the department. The department chair logs into a Kuali management system and using the permissions afforded the Payroll Supervisor role, sets the "Active to" date for Gina's membership in the Financial Assistants" group to her effective termination date, and adds Marcus as a member (with that date as the membership's "Active From" date) of the group, revoking Gina's permissions and adding the appropriate permissions and roles to Marcus' principal entity.

A somewhat more involved example...

- perMIT speaks of ASPECs with functions and qualifiers, and of copying and reassigning ASPECs to modulate privileges
- KIM and Rice speak of groups assigned to roles with memberships bounded by activity dates, and adding principals to or removing them from groups (or roles) to modulate permissions

Ongoing efforts

- We have responders for Grouper, Oracle IDM, Sun IDM, KIM, perMIT, Sakai
- May still need responders for Kuali Student, Spring Security Framework, Moodle
- Reorganizing use cases, map into XACML descriptions (and other “languages”)
- Defining APIs, demonstrating solutions in different models (Grouper, perMIT, others)

Fun URLs to Explore (and Edit, too!)

- Main Site: https://spaces.internet2.edu/display/macepaccman
- Use Cases: https://spaces.internet2.edu/display/macepaccman/Use+Cases
- Glossary: https://spaces.internet2.edu/display/macepaccman/MACE-paccman-glossary
- Comparative Taxonomy: https://spaces.internet2.edu/display/macepaccman/MACE-paccman+comparative+taxonomy
- Comparative Solutions: https://spaces.internet2.edu/display/macepaccman/Selected+Use+Cases
- API proposal: https://spaces.internet2.edu/display/macepaccman/Permissions+API+suggestion+based+on+Grouper+permissions

MACE-PAccMan Glossary and Comparative Taxonomy

ACAMP 2010

Rob Carter, Duke University