MIT Identity Services

January 2010

Scope

- Identity services and the management of identities extends to people, hosts, services, applications, and executing processes
- This presentation will primarily focus on the identity services as they relate to people

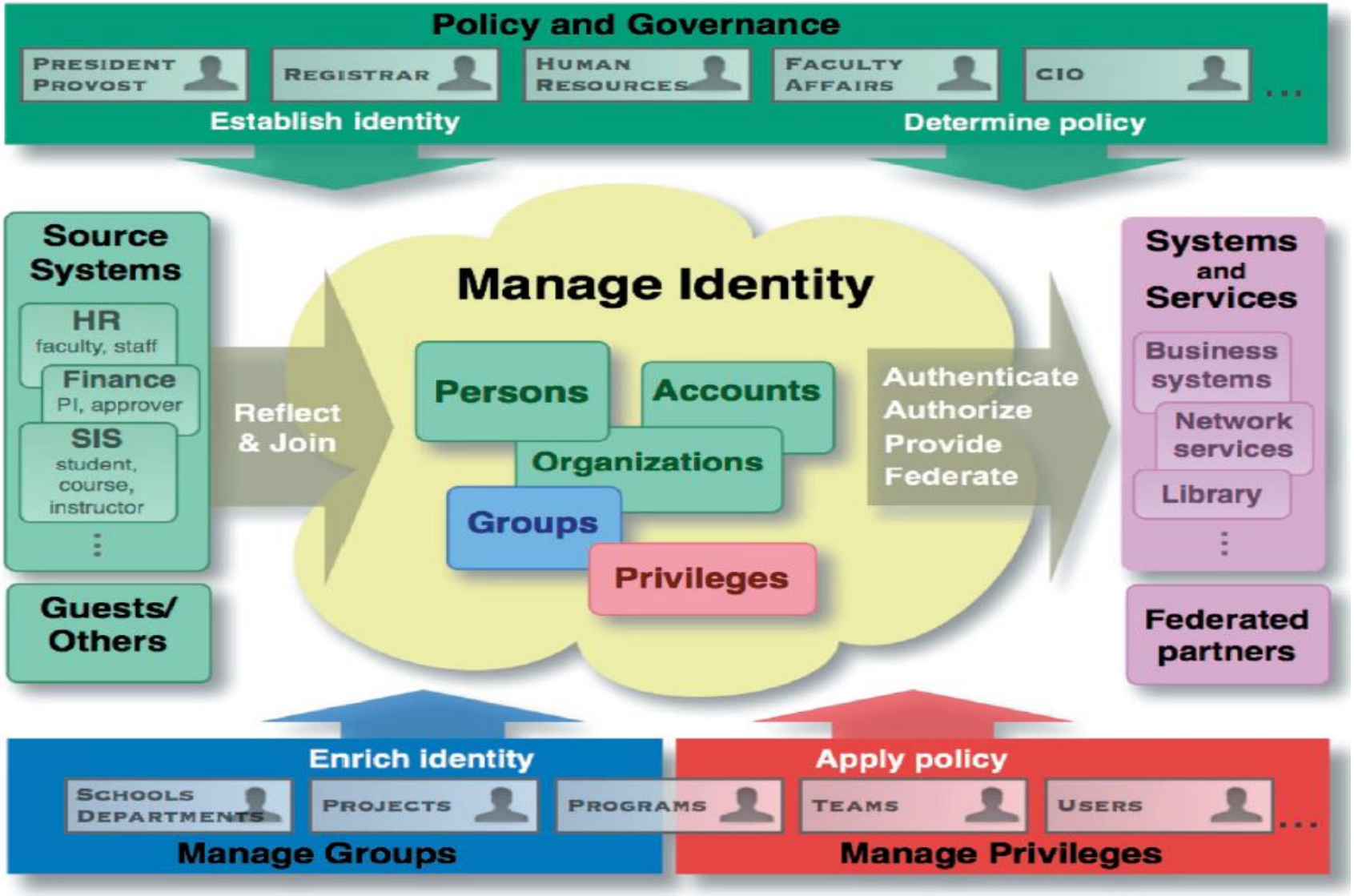
Why are Identity Services important?

- **Provisioning** - Establishes standard processes for obtaining and maintaining an MIT identity
- **Authentication** - Enable a 'real world' person to prove who he, or she, is to internal and external digital assets and resources
- **Authorization** - Ensures the distinction between registering for an MIT identity and assigning privileges to that identity
- **Compliance** - Addresses some of MIT's key privacy and legislative obligations
- **Personalization** - Enables MIT to personalize and manage the user experience
- **Branding** - Binds outstanding individuals to the MIT name, which in turn extends the brand recognition
- **Services** - Assists in maintaining and evolving a consistent information security infrastructure for access to MIT systems and data

Landscape

- People collaborate with others across traditional organizational boundaries
- Experiments may have teams that include members from dozens of organizations
- Data and other materials may be scattered across dozens of sites, organizations, or countries

Generic Components



Main Topics

- Terminology and Jargon
- Provisioning
- Authentication
- Authorization
- Data and Directory Services

Terminology and Jargon

- Moira
- MIT ID DB
- Kerberos
- Regular Account
- Special, aka sponsored, Account
- SoR
- X.509 Certificates
  - User
  - Server
- LDAP
- Federation
- InCommon Federation
- Shibboleth
- IdP
- SP
- SAML
- Collaboration Accounts
- Touchstone
- Roles
- perMIT

What is Moira?

- Moira is a meta-directory dating from 1988, originally developed for Project Athena
  - **Namespace management and reservation**
  - **User account registration and management**
  - **List and group management**
  - Network/subnet management
  - Host/Machine management
  - Athena cluster management
  - AFS and NFS file system management
  - Win.mit.edu container management

MIT ID DB and service

- The MIT ID DB provides authorized lookup and assignment of MIT ID numbers
- In 1994 MIT decided to eliminate the use of SSNs as a primary identifier across institute systems
- MIT ID DB is SoR for SSNs
- MIT ID DB does not report SSNs
- Ideally a person should only need one MIT ID number in their lifetime
- Even applicants are assigned ID numbers, prior to acceptance

Kerberos

- A computer network authentication protocol, originally developed at MIT
- Defines the MIT user namespace (e.g. mtsmith@mit.edu)
- The Kerberos protocol is generally used by native clients or thick clients, not web applications
- Kerberos authenticator lasts approximately a day
- Used in conjunction with MIT ID number to obtain MIT X.509 User Certificate

Accounts

MIT **Regular**

- employees (including faculty and staff as identified by MIT HR)
- registered students (as determined by the Registrar)
- members of the Corporation
- Members of certain Corporation or Alumni Association committees.

MIT **Special, aka sponsored**

- People not entitled through MIT affiliation to a Regular Account but who are otherwise affiliated with the Institute through activities sponsored by a current MIT faculty or staff member

Collaboration Accounts

- *Outside of the MIT namespace*
- Anyone in the world can obtain on via self-registration

Systems of Record (SoR)

- The SOR is the system that has the official master copy. Many systems have copies of data that was collected elsewhere.
- is responsible for all aspects of the integrity and maintenance of this information.
- Many systems are an SoR for only a small subset of the data that they contain
- The Data Warehouse is not an SoR

X.509 Certificates

- An X.509 certificate is an electronic document which uses digital signatures to bind together a public key with an identity
- A certificate authority (CA) issues X.509 certificates
- The MIT CA issues certs for MIT users, servers, and applications
- We also use the Equifax CA to issue some server certificates
- Certificates are generally used for web authentication. They are rarely used for native application authentication.

LDAP

- An industry standard protocol for querying and updating directory services
- Not a SoR for any MIT data
- Fed by Moira and the Data Warehouse
- Applications and systems use this as an integration tool to access names, group memberships, and other information.

Federation

- an association of organizations that use a common set of attributes, practices and policies to exchange information about their users and resources in order to enable collaborations and transactions
- each organization continues to manage its own identities, but is capable of securely sharing and accepting identities and credentials from other organizations
- Participants may use different technologies with different security approaches and still integrate their businesses without substantial custom integration.

Current InCommon Participants

A community of more than **4 million end users**.

(November 2009. Source: Higher Education Students, Faculty, and Staff, Integrated Postsecondary Education Data System.)

Higher Education Participants (143)	Government and Nonprofit Laboratories, Research Centers, and Agencies (6)	Sponsored Partners (47)
Arizona State University	Energy Sciences Network (ESNet)	Absolute Software, Inc.
Baylor University	Lawrence Berkeley National Laboratory	Apple - iTunes U
Brown University	Moss Landing Marine Laboratories	Blatant Media Corporation
California Maritime Academy	National Institutes of Health	Burton Group
California Polytechnic State University - San Luis Obispo	National Science Foundation	Cengage Learning, Inc.
California State Polytechnic University, Pomona	TeraGrid	Colorado Alliance of Research Libraries
California State University, Channel Islands		Davie County Schools
California State University, Chico		Digital Measures
California State University, Dominguez Hills		e2Campus by Omnilert, LLC
California State University, Fresno		EBSCO Publishing
California State University, Fullerton		EDUCAUSE
California State University, Monterey Bay		Elsevier
California State University, Office of the Chancellor		Good Steward Software
California State University, Sacramento		Houston Academy of Medicine - Texas Medical Center Library
California State University, San Bernardino		Identit-e
California State University, San Marcos		Internet2
Carleton College		JSTOR
Carnegie Mellon University		Kuali Foundation
Case Western Reserve University		Learn.com
Central Piedmont Community College		lynda.com
Clemson University		MCNC
College of William and Mary		Microsoft
Colorado State University		National Institute for Technology and Liberal Education (NITLE)
Columbia University		National Student Clearinghouse
Cornell University		NC Live
Dartmouth		NG Web Solutions
Duke University		North Carolina Department of Public Instruction
Emory University		OCLC
Fairfield University		OhioLink - The Ohio Library & Information Network
Florida State University		Outside The Classroom
George Mason University		PeopleAdmin, Inc.
Georgetown University		ProQuest LLC
Hampden-Sydney College		ProtectNetwork
Humboldt State University		RefWorks, LLC

IdP

- Identity Provider
  - Mediates the user's initial authentication
  - Supplies information about the user to the participating applications
  - Arbitrates what information about a user will be disclosed to a particular application

SP

- Service Provider, aka Relying Party
- This is the component that resides on the enabled application server
- Consumes the information about the user provided by the IdP
- Marshalls the disclosed information so that an application can access it
- Grants or denies access to protected content

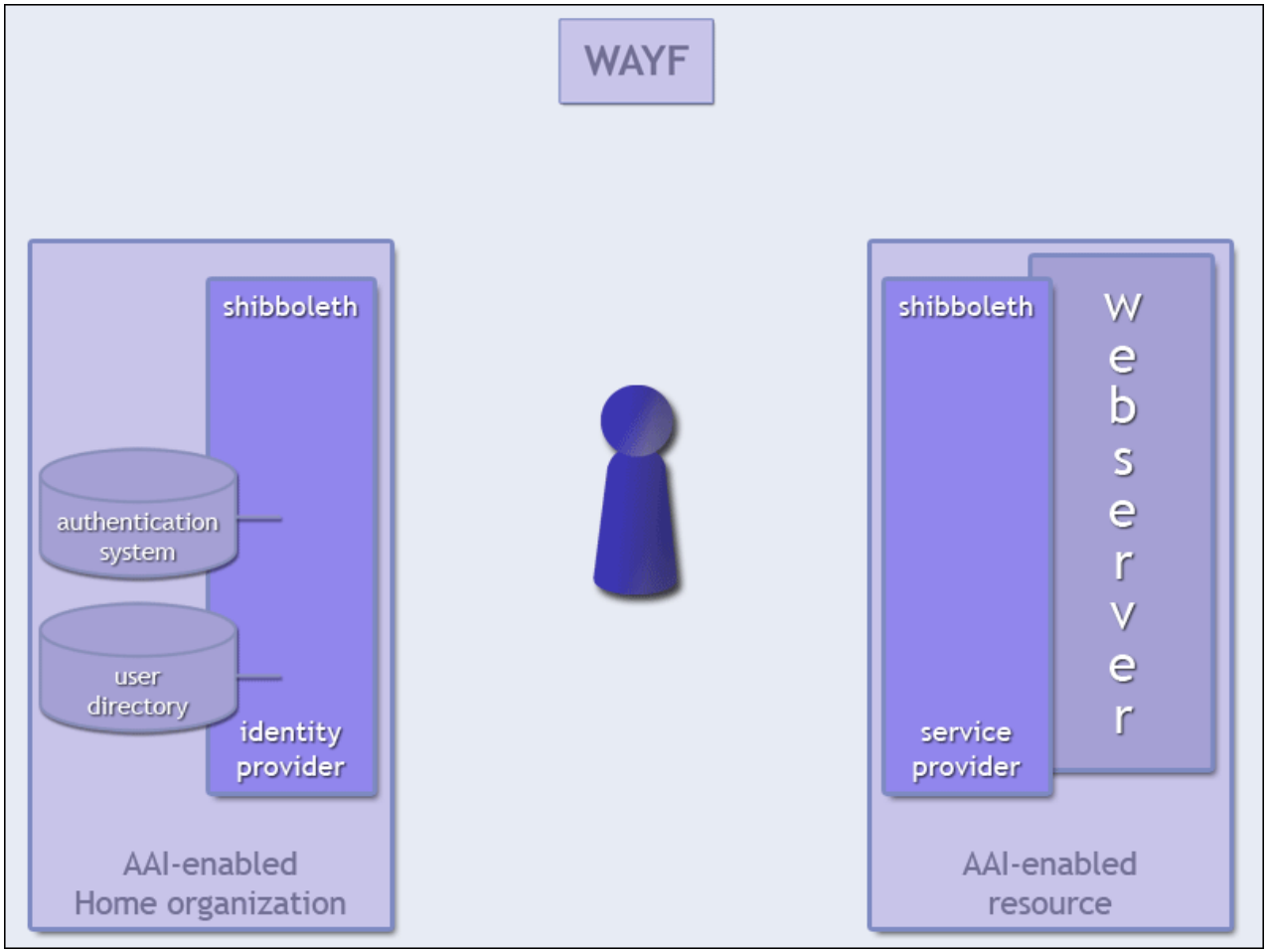
SAML

- Security Assertion Markup Language
- Standard for exchanging authentication data between an IdP and an SP
- SAML is a product of the OASIS Security Services Technical Committee
- Used by Shibboleth and many other systems

Shibboleth

- Shibboleth is a web centric authentication product
- Is a product of Internet2
- Supports federated authentication
- Uses SAML
- Interoperates with Microsoft's ADFS and Liberty Alliance compliant systems
- Includes the IdP and SP components

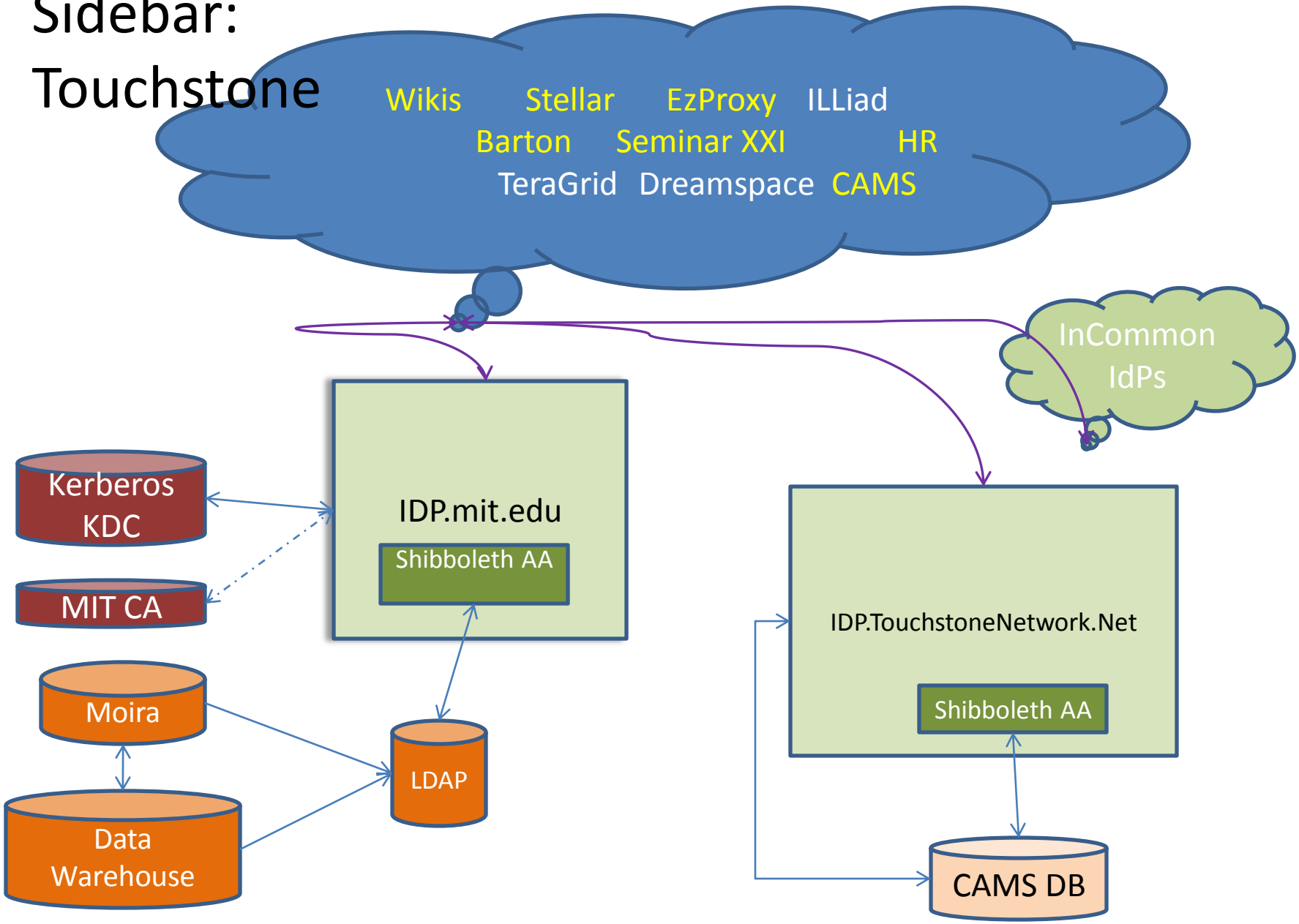
Sidebar: Shibboleth



Sidebar: Collaboration Accounts

- Outside of the MIT namespace
- Anyone in the world can obtain on via self-registration
- Used specifically for Touchstone/Shibboleth enabled web applications
- Created so that applications don’t have to create their own local account management system
- Alumni plans to migrate to this system

Sidebar: Touchstone



Sidebar: Roles

- A privilege management system developed at MIT
- in use at MIT for well over a decade
- Supports
  - Inheritance
  - Explicitly granted privileges
  - Privileges defined as the result of evaluating enterprise data
- Includes a master department hierarchy system
- Accessible via:
  - a SOAP based web service
  - Flat files
  - Exporting data to LDAP groups

Roles

- In use by over 30 applications, including:
  - Financials, payroll, student system, admissions, registrar, telephony, libraries, graduate aide, HR, environmental health and safety, data warehouse, MIT ID system, help desk, master department hierarchy, accounts management
- 6258 people have the ability to grant privileges (10/2/2009)
  - Institutional size is roughly 23,000
  - Only 601 can grant privileges if you exclude 5637 people who have the GRANT flag turned on for their privileges in the Telephony and Network category (for maintaining VoIP preferences).
- Growing interest from a number of business areas:
  - Physical security / door access / parking
  - Backup system
  - Certificate authority
  - Travel / reservations

perMIT

- perMIT is the next generation of Roles
- Roles is limited to MIT Kerberos accounts
- perMIT will allow us to manage privileges of users that authenticate via other IdPs as well
- Add strong data typing to Qualifier subtypes
  - The logic of some existing stored procedures is based on knowledge of MIT data formats, instead of data typing. This will go away.
- Expand the audit trails
- High Availability
- Make it available to other sites

Who is the MIT Community?

Provisioning

- **Identification** is the process used to determine that the person is who they claim to be.
- **Registration** is the process whereby users are given electronic credentials, ensuring that they are coupled with the correct electronic identity information. (1)

Provisioning: Key identifiers

- Let's first focus on Staff, Students, applicants, and Special Accounts:
- MIT ID Number
  - Input: Full Name, Day of Birth, optionally SSN
  - Output: MIT ID Number (2)
- Kerberos principal name
  - User chooses name and password
  - Used as the basis for most other online credentials at MIT

Provisioning: entry points

- Human Resources
  - MIT ID number, and ability to register for account
- Registrar / Admissions
  - MIT ID number, and ability to register for account
- IS&T Athena Accounts
  - MIT ID number, and ability to register for account
- MIT ID Card Office
  - MIT ID number, Library Patron ID number, and issuing of MIT ID Card

Provisioning: Open Issues

- Areas where we would like to initiate projects:
  - Level of Assurance
  - Data Quality of MIT ID number
  - New privacy concerns
  - Pylon: expose active federation users to our authorization management systems
  - Username restrictions
  - Improve management of special accounts
  - Kerberos non-null instances

Level of Assurance (LOA) (1)

- Create an application which builds the evidence to associate a Kerberos principal with a specific MIT ID Card holder.
  - When a person picks up an MIT ID Card, have the person authenticate at a workstation in the Card Office.

Improve data quality and reduce the number of times a person is assigned multiple MIT ID numbers (2)

- A new interface to the MIT ID database has been created which helps people performing data entry determine if a small typing mistake has been made. E.g. show if a newly entered SSN differs by 1 or 2 characters, while the full name matches.
- Athena Accounts is using this.
- Other systems are not yet using the new interfaces.
- Issuing multiple MIT ID numbers to the same person will be reduced by making the change to existing systems.

Privacy concern introduced by Google Apps, OpenID, and Federation (3)

- MIT usernames are being used by external systems such as Google Apps. If a DLC converts a username to a mail list, it possible for someone on the mail list to gain control of the Google App, and the data within.
- Educate people to use contact lists, not usernames, as the customer contact point for DLC business.

Expose active federation users to our authorization management systems (4)

- Create an application to facilitate the registration of active federation users with our authorization management services.
  - *Pylon* is intended to be a gateway application that will facilitate the registration of collaborators from the InCommon Federation with the MIT LDAP service and perMIT, so that application administrators may easily administer the external user's access to various application resources.
  - A person with an account from a IdP participating in the InCommon Federation would visit, or be redirected to, the *Pylon* application, which would require Shibboleth authentication. This would be done only the first time the user has accessed a participating application, such as Wikis, Stellar, or Seminar XXI.

Username restrictions

- Some systems impose length restrictions on usernames (only 8 characters)
- Create an inventory of these systems and target them for maintenance as appropriate
- Example: Roles, the perMIT work will address this issue

Improve management of special accounts

- Lack of external email address for holders of sponsored accounts
- Add new fields to Moira
- Modify sponsorship form
- Summer of 2010

Kerberos non-null instances

- Lack of central reporting for Kerberos non-null instances (root, extra, admin, …)
- This data only resides in Kerberos KDC today
- Some references are visible in Moira and other system
- Should be reflected into the Data Warehouse for reporting
- Will improve authorization management

Provisioning

- More details about provisioning can be found starting at slide number 83

Authentication

- the process of validating the credentials presented in a particular security context.
- Authentication **should** not imply access to resources, which is done with the Authorization step.

Authentication: Services and Credentials

- MIT Card Office
  - MIT ID Card
  - Prox cards for door access
- MIT Libraries
  - Library Patron Cards (sold to external community)
- IS&T
  - Small number of Secure ID Tokens
  - Small number of prox cards
- IS&T
  - Kerberos
  - MIT Certificate Authority
  - Equifax Certificate Authority
  - X.509 certificates
  - MIT Touchstone / Shibboleth
  - SAML (Security Assertion Markup Language) , part of Touchstone
  - RADIUS
  - MAC addresses

Authentication: Kerberos

- Defines the MIT user namespace
- Used in conjunction with MIT ID number to obtain MIT X.509 User Certificate
- The Kerberos protocol is generally used by native clients or thick clients, not web applications
- Kerberos authenticator lasts approximately a day

Authentication: Kerberos protocol used with

- Athena login
- Win.mit.edu login
- SAP Native GUI
- Some Jabber clients
- Some email clients
- AFS (file system) access
- Zephyr instant messaging
- Some LDAP authentication
- Active Directory
- Some CIFS/SMB (file system) access
- DLC Sharepoint usage
- Oracle SNC
- Moira, native clients
- Some SSH clients
- Some telnet and ftp clients
- PowerBuilder client access to MIT Roles
- C API interface to MIT ID system
- Optional mechanism for initial authentication to MIT IdP
- MITSIS native client
- COEUS thick client

Authentication: X.509 (soft) User Certificates

- Namespace is derived from the Kerberos name space
- Kerberos username and password and MIT ID number is used to obtain a user certificate
- Certificates tend to last approximately a year
- MIT does not currently operate a certificate revocation service (5)
- Used primarily for web authentication
- Not all devices support certificates

Authentication: Server Certificates

- Each web server that accepts user certificates, or indeed supports TLS/SSL must have a server certificate
- MIT CA is used in most cases
- Third party certificates used in a small numer of cases (Equifax) cost money

Authentication: Application Certificates

- Used to secure SOAP based web services
- Used for server-to-server authentication

Authentication: local accounts

- Many systems are written without consideration of an existing authentication infrastructure and hence implement their own local account management.
- There are likely hundreds of systems on campus doing this, including some IS&T systems.
- IS&T provides limited consulting services to integrate 3rd party software with our authentication infrastructure.

Authentication: Radius

- RADIUS is yet another widely adopted authentication and authorization service
- Used with:
  - MIT Data Warehouse
  - MIT Network Access (wired and wireless)
  - MIT Tether (PPP dial-in access)
  - iPass (to be phased out)
- Sometimes used as a way to integrate with Kerberos

Authentication: Touchstone / Shibboleth

- Primarily for web applications
- SSO
- Supports federation
- Supports multiple initial authentication mechanisms: Kerberos, X.509, password
- Passwords are never exposed to the application servers

Authentication: Touchstone/Shibboleth applications

- Stellar
- Wikis
- MIT Libraries:
  - Barton catalog
  - Interlibrary Borrowing (ILLiad)
  - EzProxy
- IS&T web site
- Seminar XXI
- Teragrid
- Microsoft Dreamspark
- Internet2 wiki
- HR Drupal site
- Roles Web UI
- Jira
- Maven

Authentication: Touchstone interest

- Alumni (~100,000 accounts)
- Koch Institute
- Industrial Liaison Program
- Other library systems
- Mathematics Department
- Other DCAD systems
- Other HR systems

Authentication: Touchstone in progress

- Transition to Shibboleth 2.x
  - Core IdP
  - CAMS IdP
  - Customer SPs (pleading and consulting)
- Phase out Stanford WebAuth
- Improve SP registration process
- Targeted ID support
- U-Approve evaluation

Authentication: Open Issues

- Areas where we would like to initiate projects:
  - In progress the Touchstone 2.0 project
  - LOA issue – see provisioning issues
  - CRL – Certificate Revocation
  - Lack of self-service creation of application certificates
  - Data Velocity issues
  - Grow the usage of Touchstone
  - TouchstoneNetwork.net InCommon membership
  - The international experience
  - OpenID

CRL (5)

- MIT uses X.509 certificates extensively and has been doing so since 1996.
- MIT does not operate a certificate revocation list (CRL) service.
- NIST is working to create a production CRL service.
- Touchstone has been working with them on testing and looking at deployment issues

Issuing Server and Application Certificates

- Currently this is a manual process involving NIST
- We desire a self-service automated process, with the authorization managed by perMIT
- Jeff Schiller of NIST has done some design work in this area

Data velocity

- Lack of realtime updates to krb_person table in Data Warehouse and Roles/perMIT
- Currently an overnight batch process
- Can lead to 3 business days before some tasks can be performed

Grow the usage of Touchstone

- Many IS&T applications wed to certificates, not Touchstone
- Identify the IS&T applications that are using certificates AND creating local accounts
- Determine budget required to update the identified applications

TouchstoneNetwork.net InCommon membership

- The CAMS portion of Touchstone is not currently a member of InCommon
- If we add it to InCommon this will add value to Alumni's and ILP's transition to Touchstone
- It also makes Touchstone more desirable to researchers involved with multi-university projects

The International Experience

- Faculty have suggested that all Touchstone pages need to support multiple languages
- Faculty are involved with international projects
- This aligns with part of MIT mission statement
- We need to budget for this

OpenID

- Should MIT become and OpenID provider as well as a Shibboleth provider?
- Privacy concerns similar to Google Apps
- What happens to a student when their MIT account goes away?

Authorization

- is the process of controlling, based on business rules, an individual's access to resources.

Authorization services

- Moira lists
  - LDAP groups
- Roles / perMIT

Authorization: Moira lists

- Can be used as mail list and access control lists
  - AFS file system
  - NFS file system
  - WIN.mit.edu AD security descriptors
  - LDAP groups
  - DLC applications
- Can contain:
  - MIT users, arbitrary Kerberos principals, external email addresses, Moira lists, machines

Authorizations: Moira lists

- Any MIT user can create a list and populate it
- A list is a simply a collection of identifiers
- A list has no privilege management semantics
- A list does not necessarily indicate what data is being protected, or exposed
  - w92all, wiki-groups, sparklerusers
- Lists do not have a full audit history

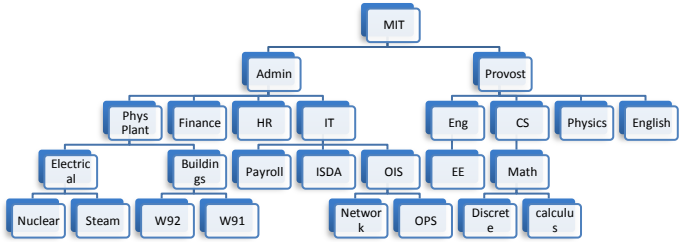
Authorization: perMIT's model

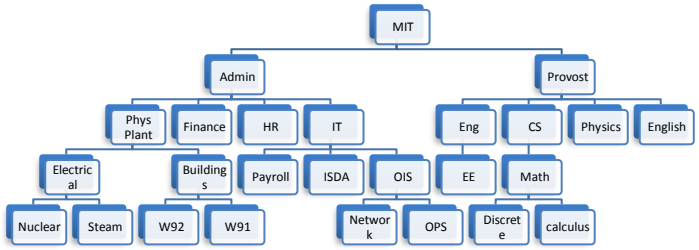
WHO

WHAT or ACTION

Related to Category
(or Application)

WHERE
(in Hierarchy)





Authorization: perMIT's model

- ASPEC = subject + function + qualifier (aka scope)
  - **Joe**
    - **Can Access** **Oxford English Dictionary Online**
  - **Jane**
    - **Can Download** **MS Office 2007**
  - **John**
    - **Can Modify Voice Mail Forwarding** **6172589850**
  - **Jim**
    - **Can Create Functions** **in category HR**
  - **Juan**
    - **Can spend and commit** **on cost object Q678543**
  - **Attila**
    - **can approve** **on cost object Q678543**

Authorization: perMIT's model

- ASPECs have starting and ending dates
  - **Attila**
    - **can approve**
    - **on cost object Q678543**
    - **Starting on July 1st, 2007**
    - **Ending on September 15, 2010**

Authorization: perMIT's model

- A subject may also be a grantor of a function + qualifier pair
- **Jane**
  - **Can grant**
    - **"Can Download + MS Office 2007"**
  - **(To anyone)**

Authorization: perMIT's model

- **A function can have child functions** (inheritance)
- EHS Coordinator for a DLC
  - Add or update Room Sets in Labs Database
  - View information on Room Sets
  - View room set info plus suppressed phone numbers
  - View EHS Training Reports
  - View all inspection data for Room Sets under a DLC
  - Maintain inspection data for Room Sets under a DLC

Authorization: perMIT's model

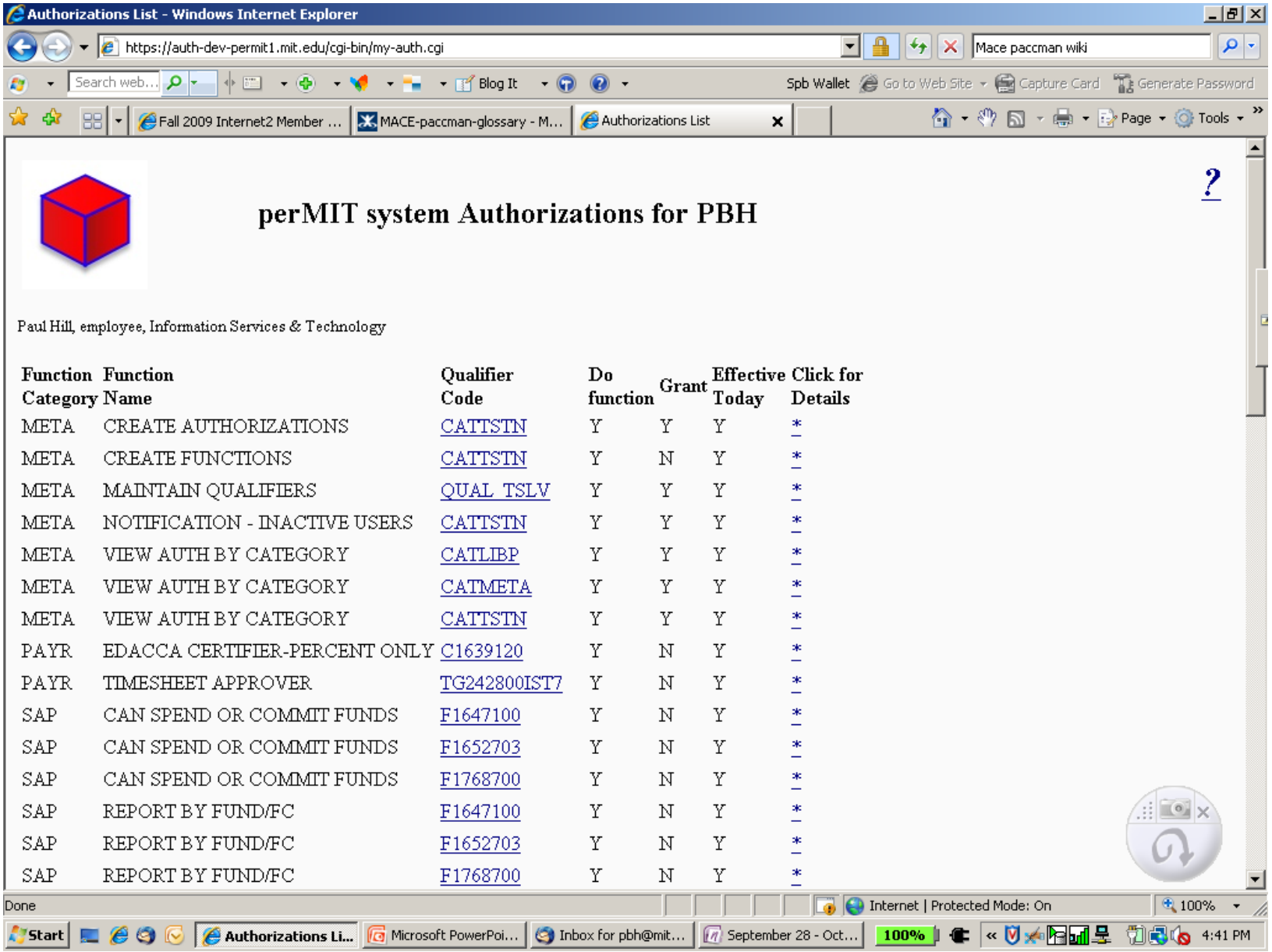
- Qualifiers are organized into hierarchies (inheritance)
- +--10000000 MIT-All
  +--10000001 Provost Area
  | +--10000005 Architecture & Planning Area
  | | +--10000267 School of Architecture & Planning (030000)
  | | +--10000270 Architecture (031000)
  | | +--10000272 Center for Real Estate (033000)
  | | +--10000273 Urban Studies & Planning (035000)
  | | +--10000275 Program in Media Arts and Sciences (036000)
  | | +--10000276 Center for Advanced Visual Studies (038000)
  | | +--10000277 Media Laboratory (039000)
  | | +--10002536 The Aga Khan Program (031500)
  | | +--10002537 Architecture & Planning - Depart Heads (030100)
  | | +--10002583 Design Laboratory (030010)
  | | +--10003158 Legatum Center for Dev Entrepreneurship (030020)
  | +--10000006 Associate Provost for the Arts
  | | +--10000604 Museum (401811)
  | | +--10000605 List Visual Arts Center (401812)
  | | +--10000606 Office of the Arts (401813)

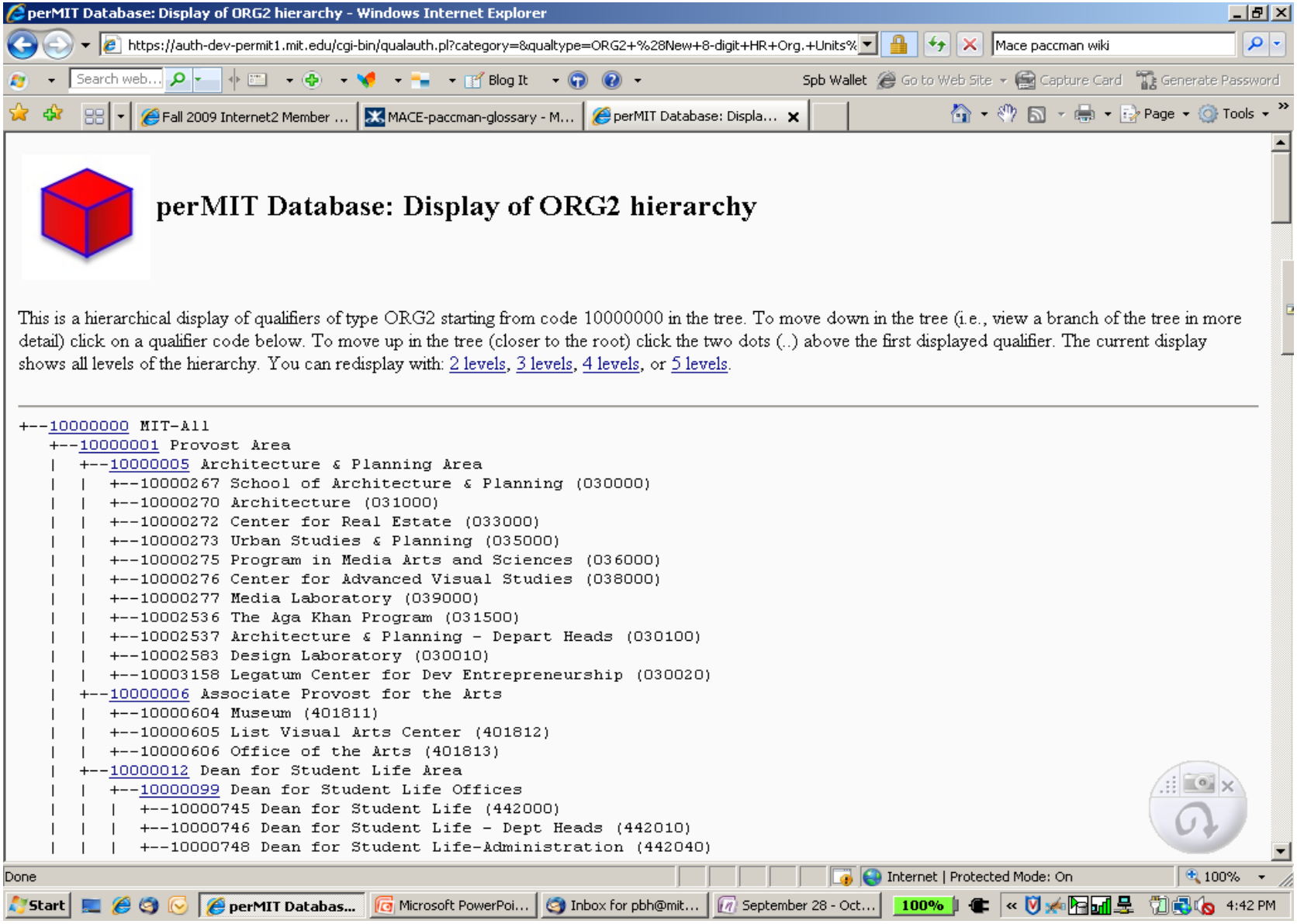
Authorization: perMIT's deployment

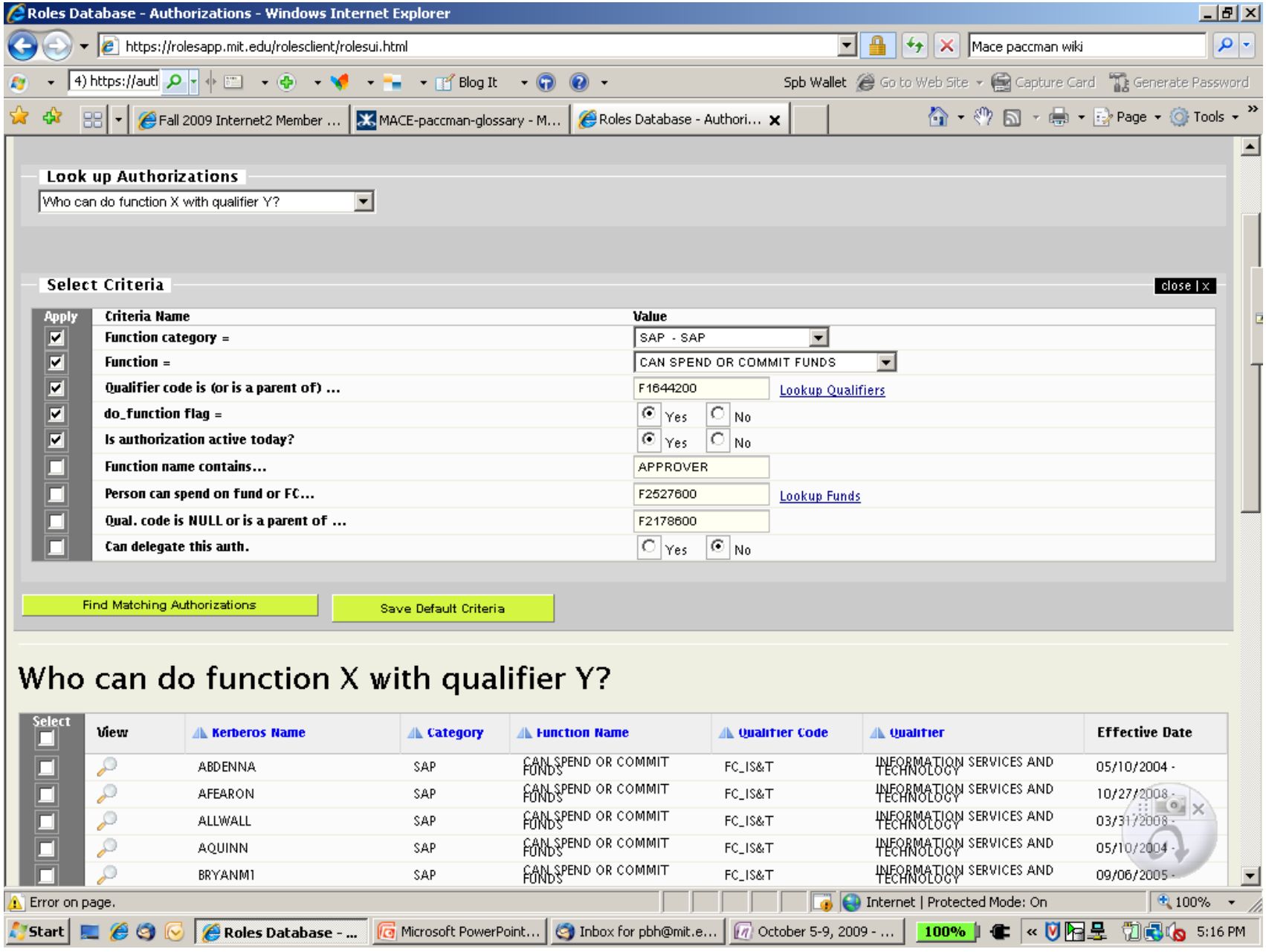
- MIT Roles has been in use since at least 1998
- perMIT is the next generation
- FY10 – perMIT and Roles will coexist, Roles will act as the master
- March 2010 – perMIT available for download to other sites
- April 2010 – some MIT applications will use perMIT as the Policy Decision Point
- FY11 – perMIT and Roles will continue to coexist, perMIT will act as the master
  - three applications have an Oracle SQL dependency

Authorization: upcoming features

- Broaden the allowable values of SUBJECTS in an ASPEC
  - Federated users, Servers / machines, Applications / processes
- Add strong data typing to Qualifier subtypes
  - The logic of some existing stored procedures is based on knowledge of MIT data formats, instead of data typing. This will go away.
- Expand the audit trails
- High Availability
- Packaging for external distribution
  - Sample data sets


Authorizations List - Windows Internet Explorer
https://auth-dev-permit1.mit.edu/cgi-bin/my-auth.cgi
Mace paccman wiki
Search web...
Blog It
Spb Wallet
Go to Web Site
Capture Card
Generate Password
Fall 2009 Internet2 Member ...
MACE-paccman-glossary - M...
Authorizations List
Page
Tools
?
perMIT system Authorizations for PBH
Paul Hill, employee, Information Services & Technology
Function Category
Function Name
Qualifier Code
Do function
Grant
Effective Today
Click for Details
META CREATE AUTHORIZATIONS CATTSTN Y Y Y *
META CREATE FUNCTIONS CATTSTN Y N Y *
META MAINTAIN QUALIFIERS QUAL_TSLV Y Y Y *
META NOTIFICATION - INACTIVE USERS CATTSTN Y Y Y *
META VIEW AUTH BY CATEGORY CATLIBP Y Y Y *
META VIEW AUTH BY CATEGORY CATMETA Y Y Y *
META VIEW AUTH BY CATEGORY CATTSTN Y Y Y *
PAYR EDACCA CERTIFIER-PERCENT ONLY C1639120 Y N Y *
PAYR TIMESHEET APPROVER TG242800IST7 Y N Y *
SAP CAN SPEND OR COMMIT FUNDS F1647100 Y N Y *
SAP CAN SPEND OR COMMIT FUNDS F1652703 Y N Y *
SAP CAN SPEND OR COMMIT FUNDS F1768700 Y N Y *
SAP REPORT BY FUND/FC F1647100 Y N Y *
SAP REPORT BY FUND/FC F1652703 Y N Y *
SAP REPORT BY FUND/FC F1768700 Y N Y *
Done
Internet | Protected Mode: On
100%
Start
Authorizations Li...
Microsoft PowerPoi...
Inbox for pbh@mit...
September 28 - Oct...
100%
4:41 PM


perMIT Database: Display of ORG2 hierarchy - Windows Internet Explorer
https://auth-dev-permit1.mit.edu/cgi-bin/qualauth.pl?category=&qualtype=ORG2+%28New+8-digit+HR+Org.+Units%
Mace paccman wiki
Search web...
Blog It
Spb Wallet
Go to Web Site
Capture Card
Generate Password
Fall 2009 Internet2 Member ...
MACE-paccman-glossary - M...
perMIT Database: Displa...
Page
Tools
perMIT Database: Display of ORG2 hierarchy
This is a hierarchical display of qualifiers of type ORG2 starting from code 10000000 in the tree. To move down in the tree (i.e., view a branch of the tree in more detail) click on a qualifier code below. To move up in the tree (closer to the root) click the two dots (..) above the first displayed qualifier. The current display shows all levels of the hierarchy. You can redisplay with: 2 levels, 3 levels, 4 levels, or 5 levels.
+--10000000 MIT-All
+--10000001 Provost Area
| +--10000005 Architecture & Planning Area
| | +--10000267 School of Architecture & Planning (030000)
| | +--10000270 Architecture (031000)
| | +--10000272 Center for Real Estate (033000)
| | +--10000273 Urban Studies & Planning (035000)
| | +--10000275 Program in Media Arts and Sciences (036000)
| | +--10000276 Center for Advanced Visual Studies (038000)
| | +--10000277 Media Laboratory (039000)
| | +--10002536 The Aga Khan Program (031500)
| | +--10002537 Architecture & Planning - Depart Heads (030100)
| | +--10002583 Design Laboratory (030010)
| | +--10003158 Legatum Center for Dev Entrepreneurship (030020)
| +--10000006 Associate Provost for the Arts
| | +--10000604 Museum (401811)
| | +--10000605 List Visual Arts Center (401812)
| | +--10000606 Office of the Arts (401813)
| +--10000012 Dean for Student Life Area
| | +--10000099 Dean for Student Life Offices
| | | +--10000745 Dean for Student Life (442000)
| | | +--10000746 Dean for Student Life - Dept Heads (442010)
| | | +--10000748 Dean for Student Life-Administration (442040)
Done
Internet | Protected Mode: On
100%
Start
perMIT Databas...
Microsoft PowerPoi...
Inbox for pbh@mit...
September 28 - Oct...
100%
4:42 PM


Roles Database - Authorizations - Windows Internet Explorer
https://rolesapp.mit.edu/rolesclient/rolesui.html
Mace paccman wiki
Look up Authorizations
Who can do function X with qualifier Y?
Select Criteria
close | x
Apply
Criteria Name
Value
Function category =
SAP - SAP
Function =
CAN SPEND OR COMMIT FUNDS
Qualifier code is (or is a parent of) ...
F1644200
Lookup Qualifiers
do_function flag =
Yes
No
Is authorization active today?
Yes
No
Function name contains...
APPROVER
Person can spend on fund or FC...
F2527600
Lookup Funds
Qual. code is NULL or is a parent of ...
F2178600
Can delegate this auth.
Yes
No
Find Matching Authorizations
Save Default Criteria
Who can do function X with qualifier Y?
Select
View
Kerberos Name
Category
Function Name
Qualifier Code
Qualifier
Effective Date
ABDENNA
SAP
CAN SPEND OR COMMIT FUNDS
FC_IS&T
INFORMATION SERVICES AND TECHNOLOGY
05/10/2004 -
AFEARON
SAP
CAN SPEND OR COMMIT FUNDS
FC_IS&T
INFORMATION SERVICES AND TECHNOLOGY
10/27/2008 -
ALLWALL
SAP
CAN SPEND OR COMMIT FUNDS
FC_IS&T
INFORMATION SERVICES AND TECHNOLOGY
03/31/2008 -
AQUINN
SAP
CAN SPEND OR COMMIT FUNDS
FC_IS&T
INFORMATION SERVICES AND TECHNOLOGY
05/10/2004 -
BRYANM1
SAP
CAN SPEND OR COMMIT FUNDS
FC_IS&T
INFORMATION SERVICES AND TECHNOLOGY
09/06/2005 -
Error on page.
Internet | Protected Mode: On
100%
Start
Roles Database - ...
Microsoft PowerPoint...
Inbox for pbh@mit.e...
October 5-9, 2009 - ...
5:16 PM

Authorization: attributes

- SAML can also contain authorization data
- E.g. is the person a student, staff, or affiliate
- Could release group membership but this becomes a huge privacy concern
- Could release application specific perMIT information with development effort

Authorization: local

- Too many applications implement their own local authorization management
- Security concern: too many dangling privileges when a person changes jobs
- Lack of consistent auditing

More details about authorization

- Can be found starting at slide 94

Data and Directory Services

- How we expose aspects of identification, registration, authentication, and authorization information to applications and systems

Data and Directory Services

- Data Warehouse
- SAML assertions via IdPs: MIT and otherwise

- (meta) Directories:
  - (Moira)
  - Hesiod
  - LDAP
  - Active Directory
    - WIN.mit.edu
    - Exchange.mit.edu
  - NIST OID
  - SAIS OID
  - CSO
  - DLC systems

Apples to Oranges

Types of MIT ID Cards

- Student
- Employee
- Affiliate
- Spouse/Partner
- DLC Sponsored
- Retiree
- Other and special
- Alumni

LDAP categories

- Student
- Staff
- Affiliate

Moira classes

- Staff
- G
- GuestYY
- YYYY
- Faculty

Notice neither card office nor LDAP have a category of “faculty”

Data Services: Open Issues

- Desire better reporting to users, of the self-service data that we have about user (host and DHCP registrations, list memberships, authorizations, …)
- One stop viewing and updates for the user
- Useful to Accounts and Security teams
- Need to scope project and make proposal

End

Provisioning Details
83

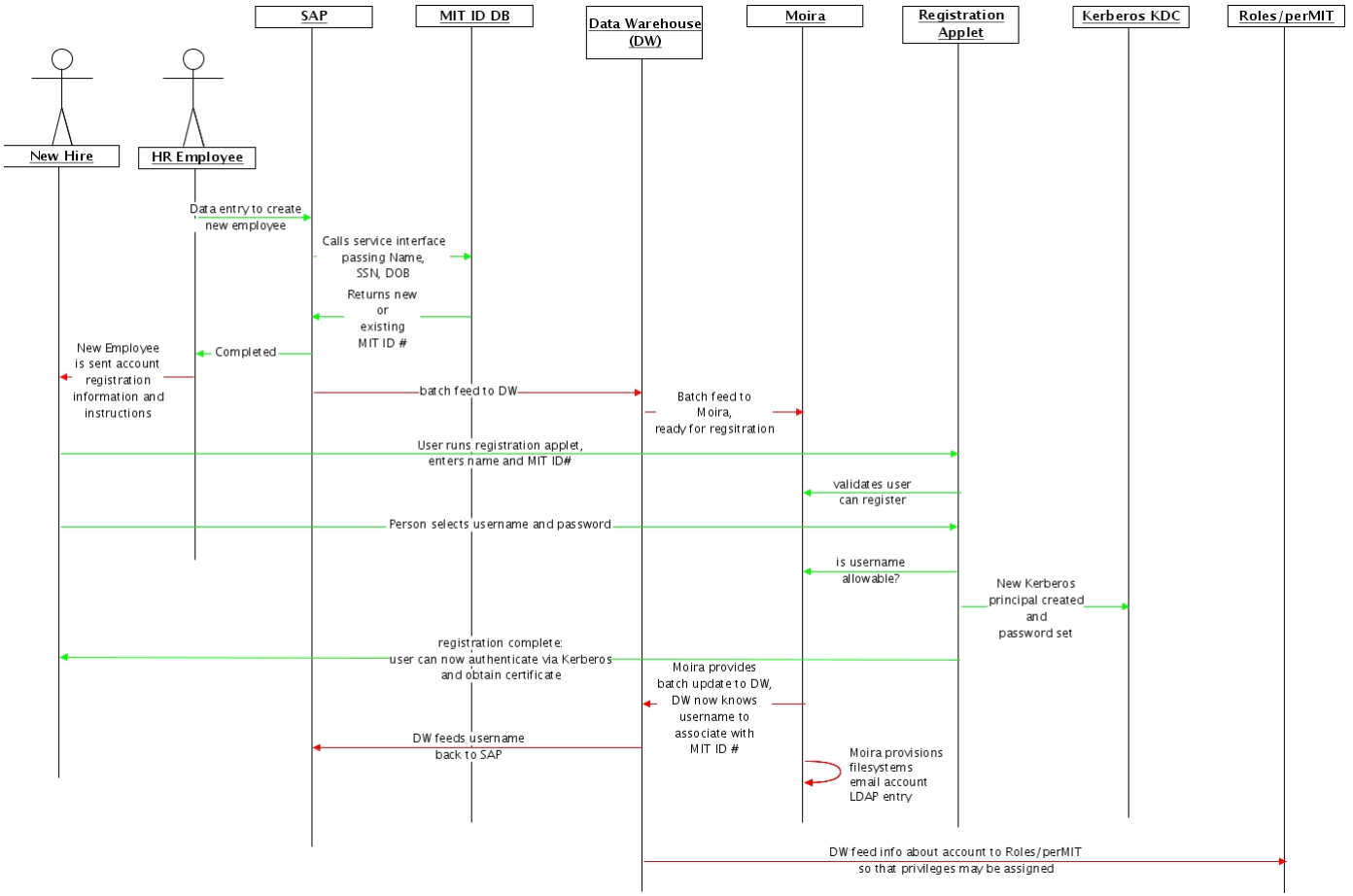
Provisioning: Systems of Record

- MITID Database
  - Entry points must first create an MIT ID Number
- Moira
  - Fed from Data Warehouse, but becomes the SoR for Kerberos Account Registration
- Kerberos
  - SoR for username and password
  - Chosen username is fed back into Moira, which then feeds it back to the Data Warehouse (KRB_PERSON) table

Provisioning: Systems of Record and entry points

- SAP/HR
  - Employees (receiving benefits, not contractors)
- Registrar/MITSIS
  - Students
- Moira
  - Affiliates (including contractors)
- Card Services
  - Affiliates, spouses and partners, DLC sponsored, …

Provisioning: example, employee



Provisioning: Special Accounts

- Any employee (provisioned by HR) may sponsor an account for someone that doesn't come through the normal processes
- Contractors, temporary employees, voucher employees, visiting scholars, visiting faculty, VIPs, friends of the institute, collaborators, …
- It is important that systems be designed so that successful authentication != authorization

Provisioning: lifetime

- MIT ID Numbers by design are never recycled
- Ideally a person should only need one MIT ID number during their lifetime (2)
- Kerberos principal names were originally intended to be recycled, and were for many years.
- At this time Kerberos principal names are not recycled. (3)

Provisioning: non-Kerberos accounts

- When dealing with systems that support federated authentication, or distributed authentication, there is a registration aspect of provisioning which is bound to the authorization process.
- External users that are actively using MIT applications **should** appear in our central authorization management systems. (4)

Provisioning: Collaboration Accounts

- All (self registered) Collaboration Accounts are propagated into Moira and LDAP and MAY appear on Moira and LDAP lists and groups.
- At this time, Collaboration Accounts, cannot be represented in Roles/perMIT authorizations. This will change as perMIT reaches production status.

Provisioning: Accounts from federation partners

- Accounts from federation partners do not automatically appear in Moira or LDAP. (4)
- This presents some usability issues for some applications.

Authorization
94

- Further details

Authorization: perMIT's model

- Each function is associated with a particular type of qualifier
- The function "Initiate a Termination Request"
  - Can have a qualifier of ORG Unit (e.g. Department of Athletics, Community Programs)
  - Cannot have a qualifier of Payroll Deduction Type (e.g. Day Care Deductions)

Authorization: perMIT's model

- **Functions have an attribute which determine to which category they may be applied**
- Example of Functions within category "Telephony and Network"
  - Administer phone preferences by network ID
  - Can administer telephones authorized by phone no.
  - Network Administration
  - Telephone administration
- The functions above fall within category "Telephony", not "Student Financial Systems". Thus, users or applications that are limited to granting or viewing ASPECs within the "Student Financial Systems" category would not have access to the above functions.

Authorization: perMIT's model

- **More than one qualifier type can exist within a category**
- Functions within category "Telephony and Network"
  - Administer phone preferences by network ID
    - Applicable qualifier type = **Network IDs**
  - Can administer telephones authorized by phone no.
    - Applicable qualifier type = **MIT Phone numbers**
  - Network Administration
    - Applicable qualifier type = **COST OBJECT**
  - Telephone administration
    - Applicable qualifier type = **COST OBJECT**

Authorization: perMIT's model

- Rules / Implied privileges
- Added after over a decade of deployment

Institutional Data from a variety of systems of record

+

Simple set of rules

=

ASPECs for a large number of users

- Access to library resources
- Door access controls

Authorization: perMIT's model

- Master department hierarchy
  - Is conceptually independent of perMIT
  - Is bundled with perMIT
  - Is used by perMIT, and other systems
- used for is creating a master hierarchy whose objects can then be linked to the department-like objects in the various stovepipe hierarchies
  - Lets you relate or link one vertical view with another
    - HR org, Academic units, profit centers, spending groups, …