Three Case Studies in Access Management

IAM Online
June 10, 2015 - 2 pm EDT

Andy Morgan, Oregon State University

Mandeep Saini, GÉANT

Albert Wu, UCLA

Moderator: Tom Barton, University of Chicago

Fit for Purpose?

These case studies provide a glimpse into the types of access management problems our community needs to manage, and how well two of our community developed tools are suited to the task

- Grouper (and COmanage, too, for one case study)

They manage the problems and little else could, but . . .

- Do they have all desired functionality?
- Are they easy enough to use?

Grouper

Andy Morgan

Access Management Strategy

- Historically, each application/service received their own version of reference data from which to make access decisions
- Duplication of effort

Goals

- One version of the truth for reference data
- Synchronize same data to multiple directory services
- More efficient reuse of reference data

Reference data based groups

Move away from custom scripts to populate AD and LDAP groups

- Grouper allows mixing of reference data with ad hoc
- Friendly interface to manage exceptions
- Easily allows same group in AD, LDAP and Google
- No custom scripting for each group
- Examples
    - Student athlete printing
    - Aruba ClearPass Management
    - Mailing list memberships

PAC-12 video for on-campus residents

Provide access to PAC-12 video network to on-campus residents

- Load resident location from Housing database into Grouper using SQL loader
- Combine all the resident hall groups into one group named *pac12tv*
- Provision the *pac12tv* group in AD and LDAP using the PSP
- Read LDAP *ismemberof* attribute into a scripted attribute resolver in Shibboleth
- Release the entitlement attribute to the SAML SP authentication gateway used by PAC12 streaming service

Course groups

Populating course groups into Canvas, AD, LDAP and Google

- Requirement for frequent (or real-time!) updates of enrollments from Banner into Canvas
- SQL Loader enrollment jobs run about an hour
- Real-time updates will require some event-based processing from Banner to Grouper
- Canvas not utilizing Grouper today, but functionality still desired

Grouper PSP (Provisioning Service Provider)

- Creates groups in LDAP and Active Directory
- Really complicated configuration - multiple XML files
- Not clear how the various config snippets connect together
- We are looking forward to the new message-queue based provisioning in the next version of Grouper

Google Apps Grouper Provisioner

Allow delegation of group creation to departments and individuals, and provide ability for data-driven groups

- Provisions groups and group membership into Google
- Written by Unicon for OSU
- Open-source
- https://github.com/Unicon/googleapps-grouper-provisioner

Oregon State UNIVERSITY

GÉANT Access Management Story

Mandeep Saini

InCommon IAM Online

10th June 2015

Introduction

- GN4 - a 7 year project under Horizon 2020
  - Requires a robust and efficient solution for all aspects of identity management.
- GÉANT Community
  - Virtual Organisation
- VO Authentication
  - eduGAIN service
  - Successfully addresses authentication in heterogeneous environment.
- VO Authorisation
  - Multiple services, each with local database to store groups and authorisation attributes.

Problem Statement

- Distributed authorisation leads to …
  - Duplication of data
  - Duplication of effort
  - Increased risk of stale data
  - Complex centralised user provisioning and deprovisioning process
  - Audit ineffectiveness

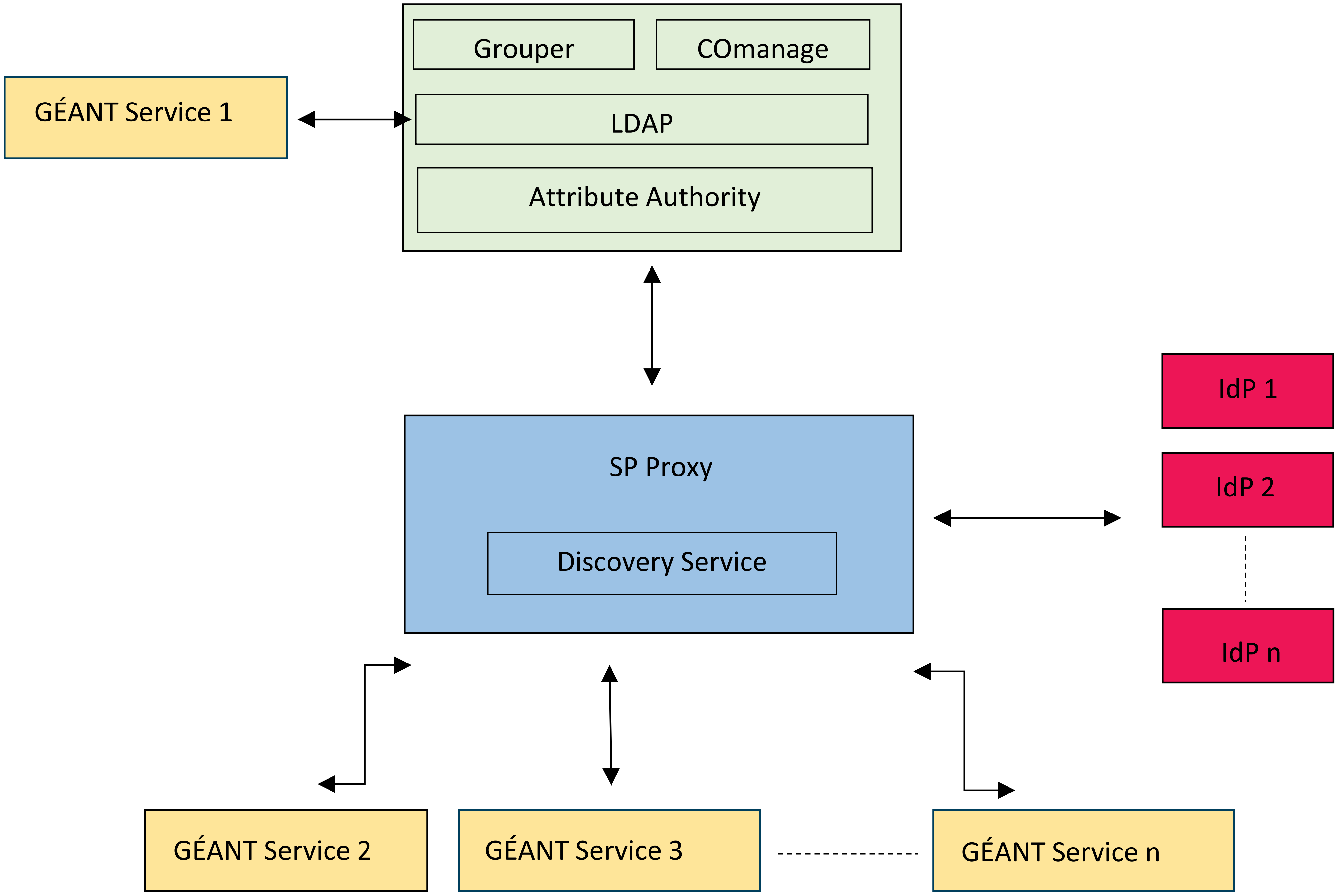
Proposed Solution

- Central Authorisation Management System
  - Centralises authorisation data
  - Decentralises the management for authorisation data
  - Defines workflows for the effective data management and people management

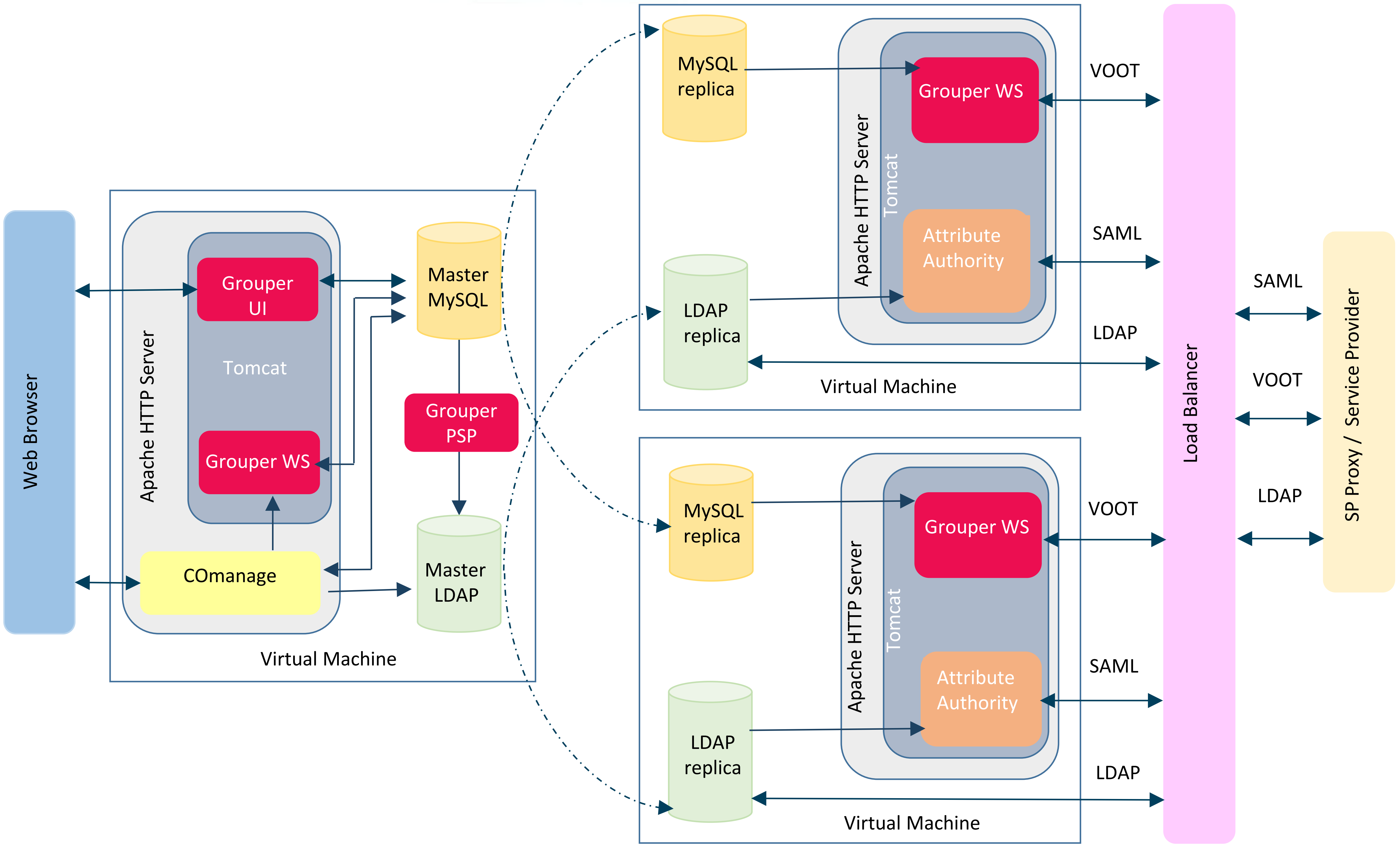
Workflows

- Bootstrapping using delegation model
- Adding/Removing a project participant
- Change of Affiliation
- Change of group membership
- Project participant accesses a service for the first time, who is not registered in central system.
- Revalidating project participants
- Managing exceptions
- Auditing

High Level Architecture



High Availability Architecture



Current Status

- GÉANT CAMS rolled out in production in April 2015.
- Used bootstrapping workflow to register GN4 Phase 1 project participants.
- GN4 Intranet (SharePoint 2013) using CAMS for authorisation
    - Grouper Claim Provider
        - Uses VOOT Connector
        - Queries Grouper to add search capabilities to the people picker.
    - LDAP Attribute Store
        - Provides user’s authorisation data at login time.

Challenges and Lessons Learned

- No single product covers all use cases out of the box.
- All VO’s are unique with different requirements.
- Product usability needs improvement.
- User training is important.
- Define group & OUs structure in advance.
- Decentralisation requires user buy-in.

Next Steps

- GÉANT SP Proxy’s integration with CAMS.
  - GÉANT Wiki
  - GÉANT Tools Portal
  - GÉANT JIRA
  - Other GÉANT Services
- Automation of remaining workflows:
  - Project participant accesses a service for the first time, who is not registered in CAMS.
  - Revalidating project participants
  - Managing exceptions
  - Auditing
- Retrieval of user’s group membership using EPPN via VOOT Connector.

Thank you

mandeep.saini@geant.org

GÉANT

Networks · Services · People

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

Grouper-Powered Roles and Access Management

Internet 2 IAM Online

June 10, 2015

Albert Wu

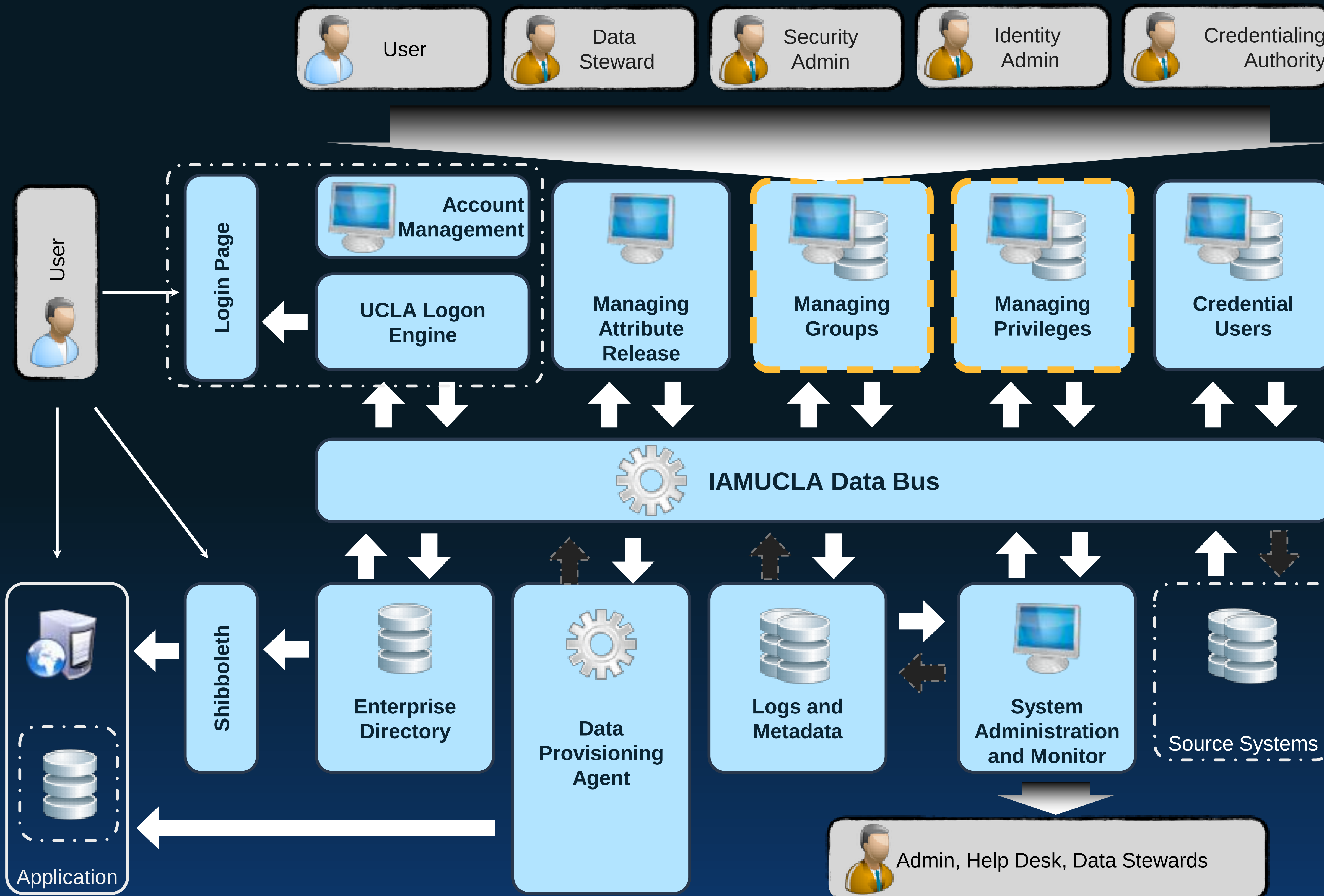
UCLA: Grouper Everywhere

Grouper is a key strategic component of UCLA's identity management service (IAMUCLA).

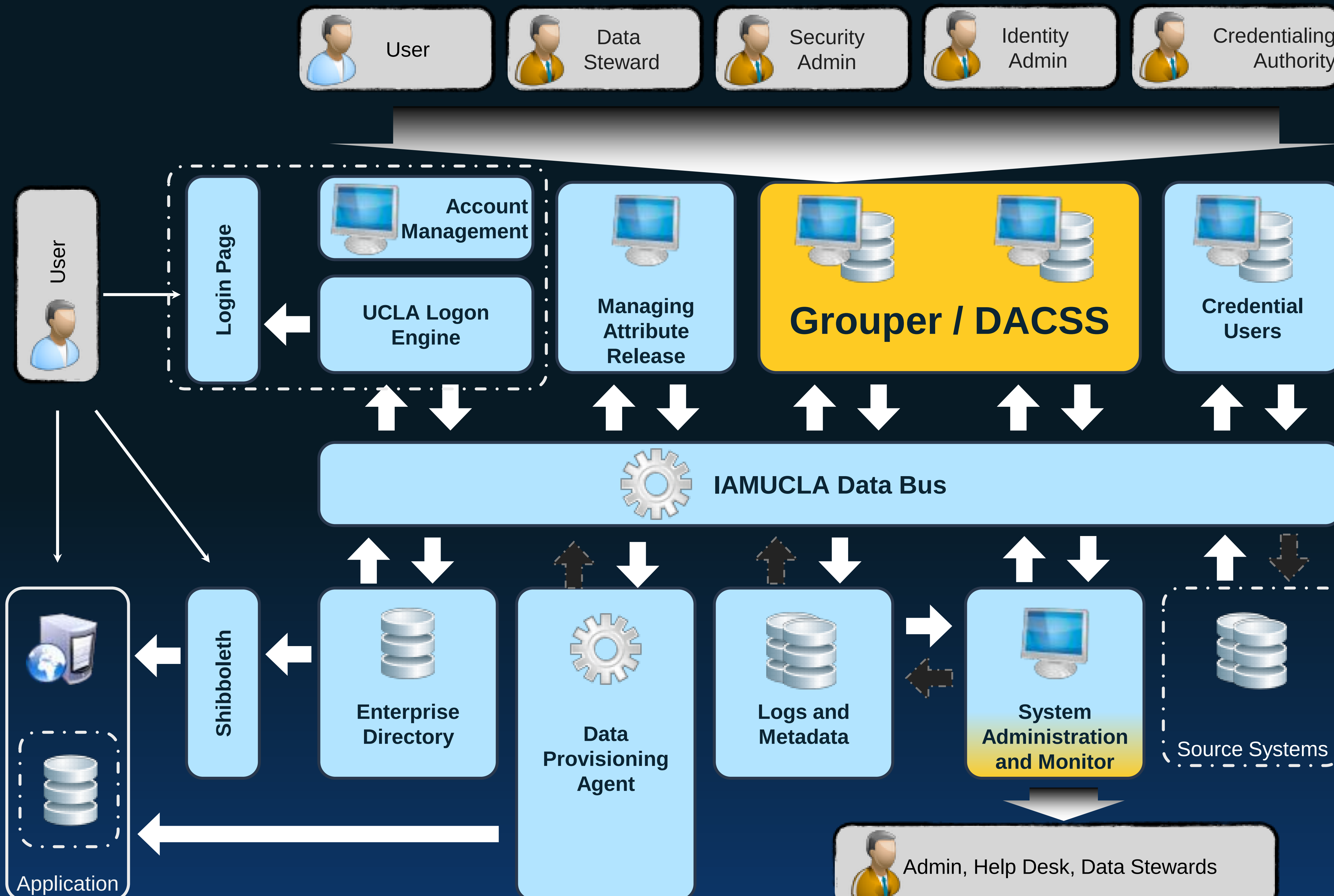
Where as Shibboleth is our choice for Web SSO across over 650 UCLA applications, Grouper is our platform of choice for enterprise role/group management. We want to connect Grouper to all UCLA electronic services.

Leverage community effort and expertise; Promote standards adoption and reuse.

IAMUCLA Architecture Roadmap



Grouper as a strategic IAM Component



Grouper Deployment Strategy

Administration	Data (Taxonomy)	Technology
• Delegate Administration • Adopt and evolve organically • Build data steward partnerships	• Define high level group taxonomy • Create group naming and delegation mechanism • Evangelize best practice	• Focus on scaling from the very beginning • Promote adoption among developer community • Integrate Grouper seamlessly with other IAMUCLA services

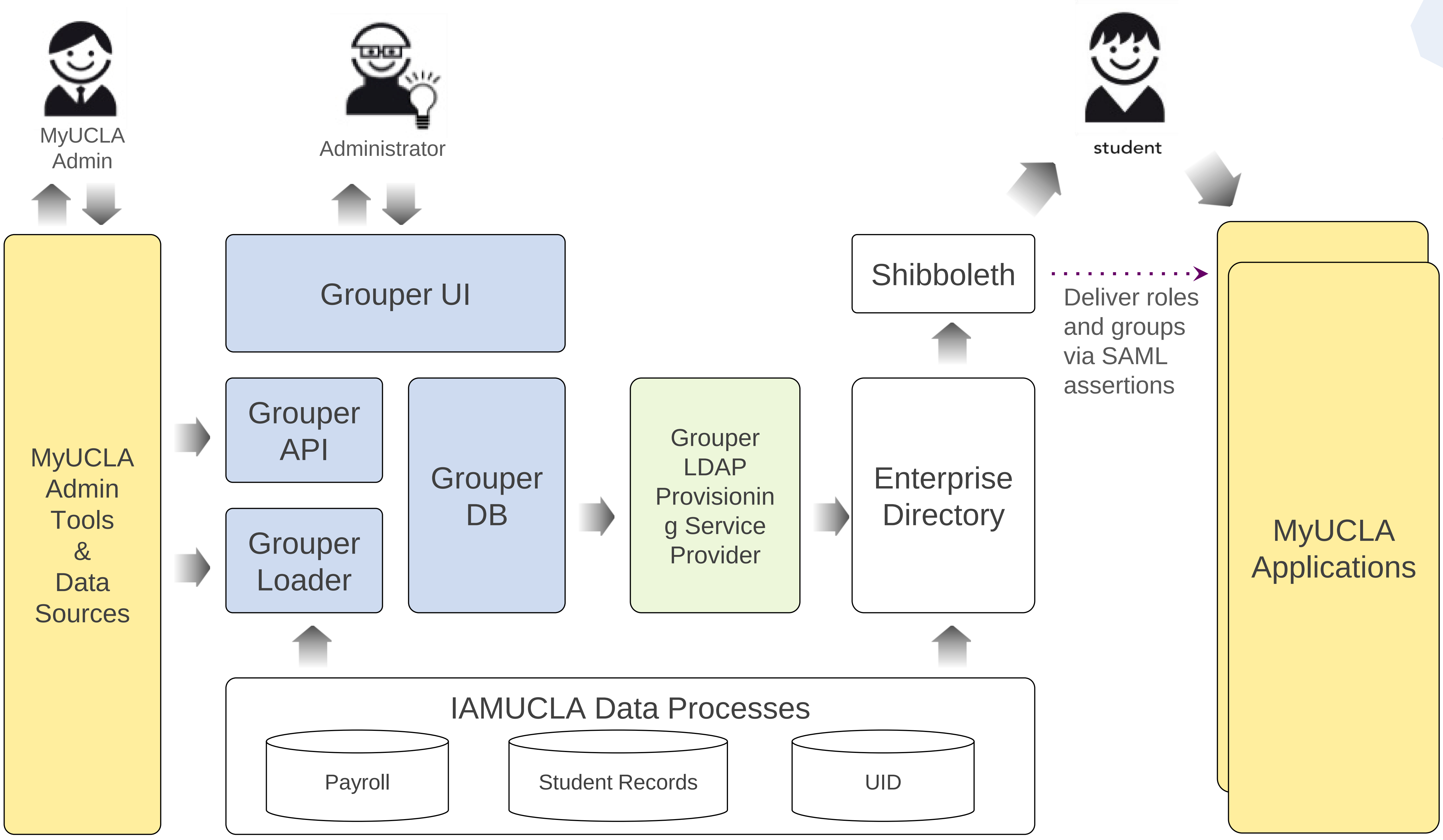
Use Case: MyUCLA

- UCLA’s Student Service Portal
- MyUCLA not a single system. Rather, it is a collection of web services and web applications tied together with common branding, navigation, workflow, and security/access control.
- A joint development effort among Student Affairs, College of Letters and Science, and IT Services.
- Grouper and Shibboleth are its role-based access control module, serving 50,000+ users, 70+ roles, and dozens of applications

MyUCLA Groups and Roles

- Defined and maintained by MyUCLA teams
- “Enterprise” Roles
  - Automated data updates from book-of-record systems
  - Mostly determine broad-level feature access
  - e.g., new-admits; graduate-students;
- “Local” Roles
  - Maintained by MyUCLA Administrators
  - Used for ad-hoc work group or staff access
  - e.g., counselors; student government election committee

MyUCLA / Grouper Integration



Lessons Learned from MyUCLA

- Changing Developer mindset to adopt common role management solution isn't easy, but it is critical for long term success
- Empowering applications to manage their own groups by delegating group registration is key to growing adoption
- Rapid access provisioning and deprovisioning at large scale still needs performance tweaks
- Data definition work (e.g., what is a "student") needs to happen in parallel with technology implementation – Having data steward participation is priceless

Use Case: BruinCard

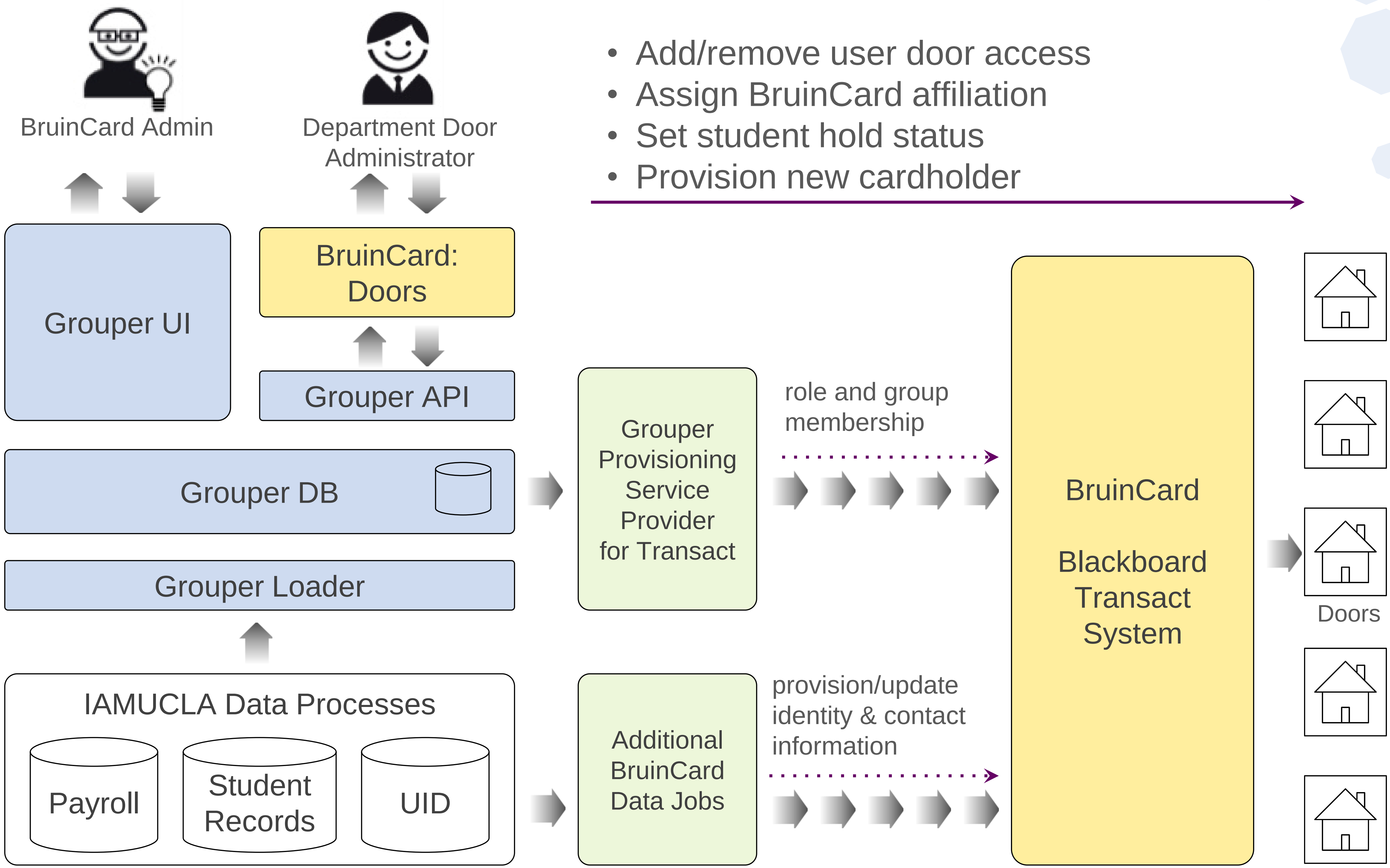
- BruinCard: ID card, debit card, and door access key
- Over 100,000 active card holders accessing approximately 800 doors / door groups across 39 buildings
- Door access management is delegated to 40 plus participating departments
- Vendor system (Blackboard Transact) isn't built to handle large scale delegated administration
- Using Grouper to simplify and automate door access provisioning/de-provisioning
- *UCLA is not alone. Duke University also integrated Grouper and Blackboard Transact in similar ways*

BruinCard Groups and Roles

- Manage employee and student door access
  - Grouper Group => Door Access Group
  - Build simple door management UI for departmental door admins
  - Use institutional data to automat access provisioning/de-provisioning (e.g., all medical and dentistry residents have access to lounge; all student and employee have after hour access to library)
- Provision cardholder campus affiliations and dining discount program eligibilities

Managing BruinCard via Grouper

- Add/remove user door access
- Assign BruinCard affiliation
- Set student hold status
- Provision new cardholder



Lessons Learned from BruinCard

- Grouper math (ability to perform and, or, except operations) made formulating (and changing) complex groups easy.
- When done right, a purpose-specific user interface simplifies group management for non-technical, administrative staff while harnessing all the automation behind the scene
- Demand for real-time access management is higher than we anticipated. Need to further develop real-time event triggered changes (More API, less Loader)

Other Grouper Uses

- Service Entitlement
  - PAC-12 TV Access
  - HBO GO
  - Google Apps for Education
  - Gartner
  - Lynda.com
  - More…
- Consolidate organizational group management
  - Active Directory
  - Web CMS
  - Email Distribution Lists
  - Service Management and Development Tools

Next Steps

- Improve API performance
- Better documentation
- Broaden adoption among existing applications
- Cloud services integration

Evaluation

Please complete the evaluation of today's webinar

https://www.surveymonkey.com/s/IAM_Online_June_2015

InCommon Shibboleth Installation Workshops

September 17-18, 2015 – DeAnza College, Cupertino, CA

October 19-20, 2015 – University of Texas-Arlington

Registration is open at www.incommon.org/shibtraining

Upcoming Events

Upcoming IAM Online webinars

July 8, 2015 - IAM Online

Case Studies - InCommon Certificate Service

www.incommon.org/iamonline

October 4-7 – Technology Exchange, Cleveland, OH

https://meetings.internet2.edu/2015-technology-exchange/