Tom Barton

University of Chicago

Towards Common Identity Services

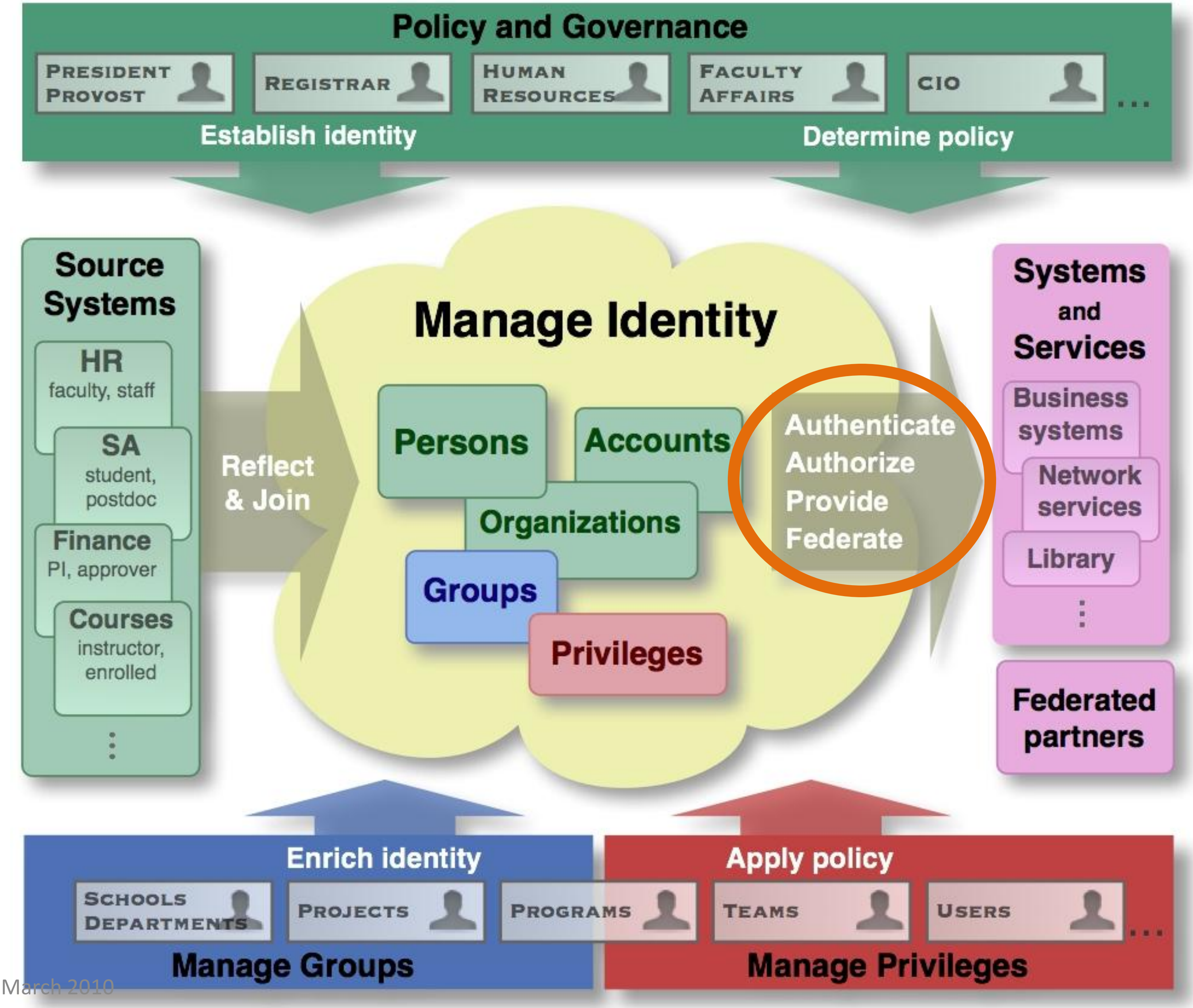
- Consortium of universities building an enterprise-level, easy-to-install open source podcast and rich media capture, processing and delivery system.
- Typical security issues need to be handled
  - User authentication
  - Service authentication
  - Proxy authentication
  - Long-running processes
- Current choices
  - ***Integration with enterprise services***
  - ***Out-of-the-box support for enterprises lacking those services***

“Is this a problem that the Matterhorn software needs to solve?

… I hope we can come up with a cheap & easy solution in order to get on with our fundamental tasks involving the handling of media.”

Josh Holtzman, Matterhorn Team member

opencast list, May 15, 2009



Policy and Governance

President Provost

Registrar

Human Resources

Faculty Affairs

CIO

…

Establish identity

Determine policy

Source Systems

HR
faculty, staff

SA
student, postdoc

Finance
PI, approver

Courses
instructor, enrolled

⋮

Reflect & Join

Manage Identity

Persons

Accounts

Organizations

Groups

Privileges

Authenticate

Authorize

Provide

Federate

Systems and Services

Business systems

Network services

Library

⋮

Federated partners

Enrich identity

Schools Departments

Projects

Programs

Teams

Users

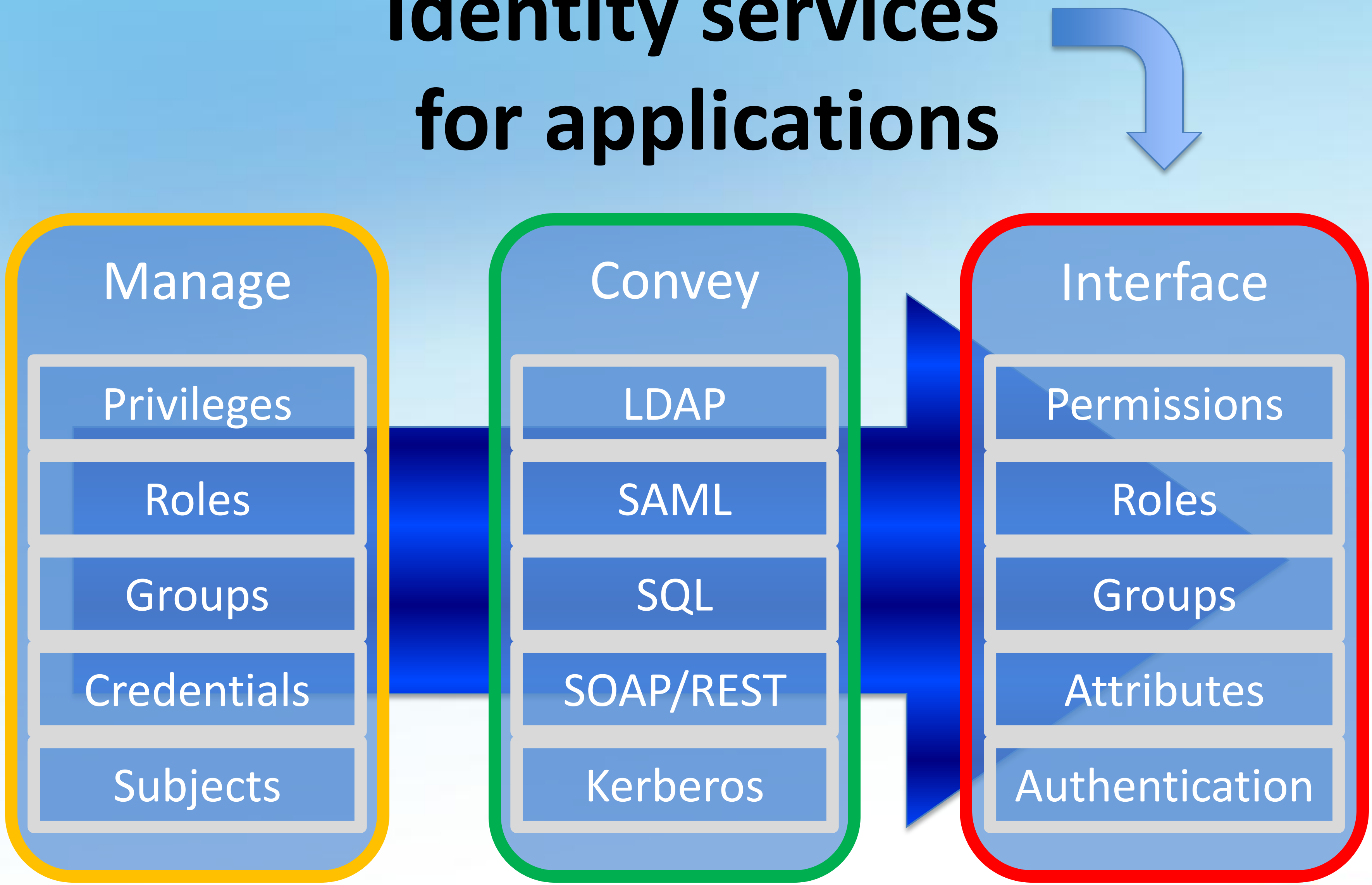
…

Apply policy

Manage Groups

Manage Privileges

Identity services for applications



Manage

Privileges

Roles

Groups

Credentials

Subjects

Convey

LDAP

SAML

SQL

SOAP/REST

Kerberos

Interface

Permissions

Roles

Groups

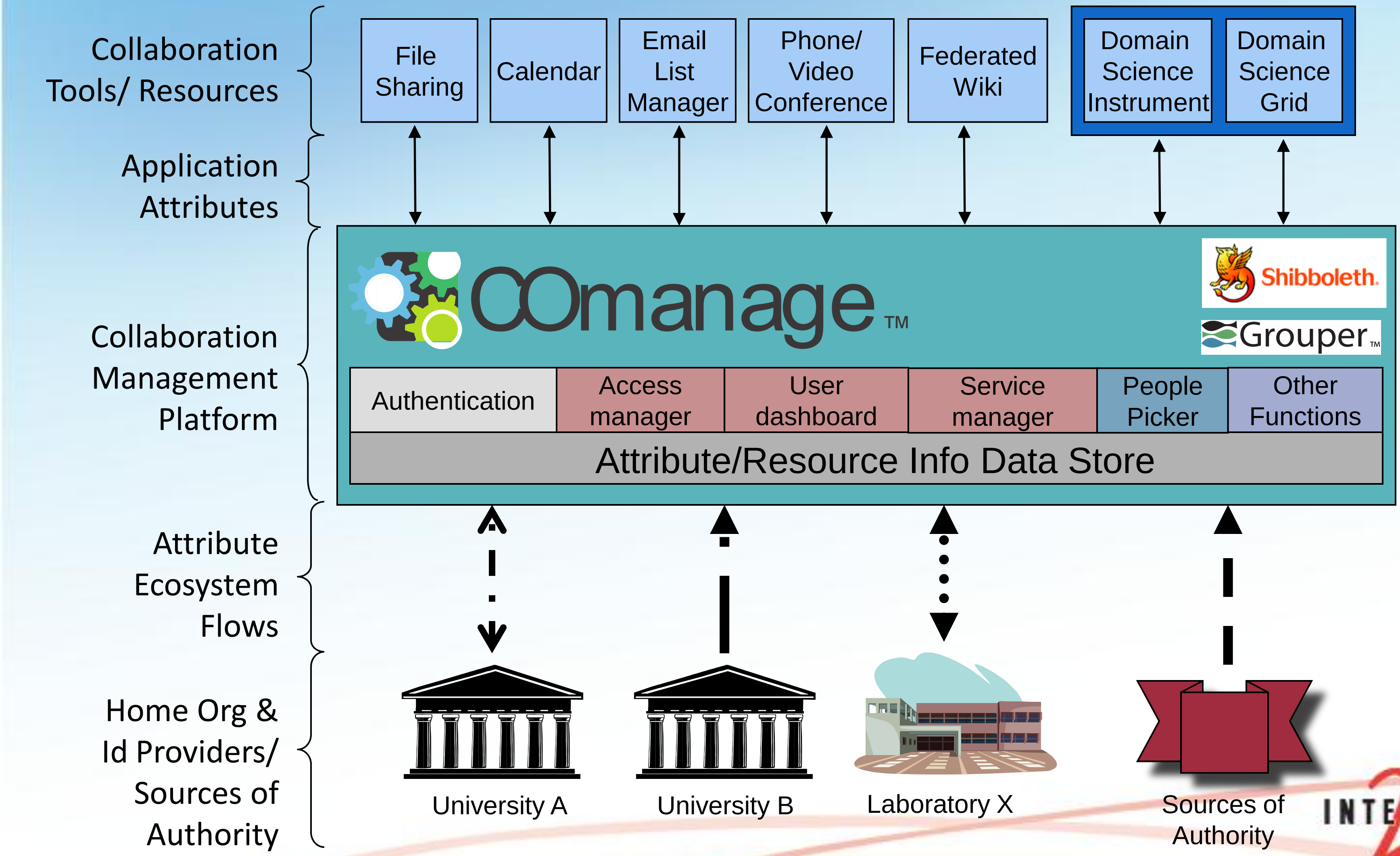
Attributes

Authentication

Scientific & scholarly collaborations

- Groups of academics share private drafts of papers, data sets, etc among themselves and eventually release reports, papers, etc to the community
- Typical needs
  - Document sharing
  - Scheduling
  - Email list
  - Colleagues span several organizations
- Current choices
  - ***Run own collaboration-specific wikis and accounts***
  - ***Use GoogleApps and accounts***

Collaboration Management Platform and the Attribute Ecosystem



Collaboration Tools/ Resources

File Sharing

Calendar

Email List Manager

Phone/ Video Conference

Federated Wiki

Domain Science Instrument

Domain Science Grid

Application Attributes

Collaboration Management Platform

COmanage™

Shibboleth.

Grouper™

Authentication

Access manager

User dashboard

Service manager

People Picker

Other Functions

Attribute/Resource Info Data Store

Attribute Ecosystem Flows

Home Org & Id Providers/ Sources of Authority

University A

University B

Laboratory X

Sources of Authority

WANTED:
Domesticated applications

- User centric identity, not tool-based identity

- Internet2's COmanage
- SURFnet's COIN; services spanning access management
- Sympa as VO manager
- SWITCH
- Duke
- Clemson
- Bamboo
- CLARIN

Common integration need: Identity Services

- Enterprise applications
  - Matterhorn
  - uPortal
  - SAKAI
  - Kuali
- Scholarly collaboration
  - General collaboration applications
  - Domain-specific tools

June 2009 Advanced CAMP: Identity Services Summit

- Participation
  - Open source project developers
    - Jasig (uPortal, CAS, Bedework)
    - SAKAI
    - Kuali
  - Campus developers & architects
  - Internet2/MACE
  - Kantara Initiative
- Project reviews (surveys & sessions)
- Lightning talks, break-outs

Some action items from the first Identity Services Summit

- Access management glossary and mapping between open source projects
- KIM – Grouper service implementation proof of concept
- uPortal – Grouper service implementation proof of concept
- Shibbolized & CASified .NET & sharepoint
- Bedework & COmanage discovery
- Enhance development frameworks with roles, etc.
  - Spring, django

Emerging domestication approaches

- SAML: authentication & attributes
  - Containers & frameworks, php, java, python, .NET
- OpenSocial's "social data" API
  - Person, Groups, Attributes (AppData)
- API-to-API mappings
  - Google: SURFnet, USC, Brown
  - Kuali Identity Management: LDAP, AD, Grouper
  - uPortal: LDAP, RDBMS, Grouper
- Leverage LDAP integration
  - COmanage Proof of Concept

MACE-Paccman: some problems

- Access Management terminology is confusing e.g. privilege, permission, entitlement, authorization
- Access Management is often embedded in applications and so is reinvented often
- Access Management often does not account for federations
- Provisioning is easier than de-provisioning
- Audit trails are often per application if they exist at all

Paccman slides courtesy of Tom Dopirak

MACE-Paccman Initial Deliverables

- Glossary and models for Access Management
  - How to use groups
  - How to use privileges
  - How to provision embedded Access Management software
  - Audit Considerations
- Comparative glossary with major access management endeavors and Open Source Higher ED projects e.g. Sakai, uPortal, Kuali
- Use Cases in Access Management
- Mapping use cases to existing efforts
  - Kuali KIM
  - MIT’s perMIT
  - Internet2’s Grouper

Kuali Foundation

"open source administrative software for higher education, by higher education"

- kuali financials
- kuali coeus (research administration)
- kuali student
- kuali rice (middleware framework)
- Incubation projects
  - ole (integrated library system)
  - continuity planning
  - payroll/hr
  - materials management

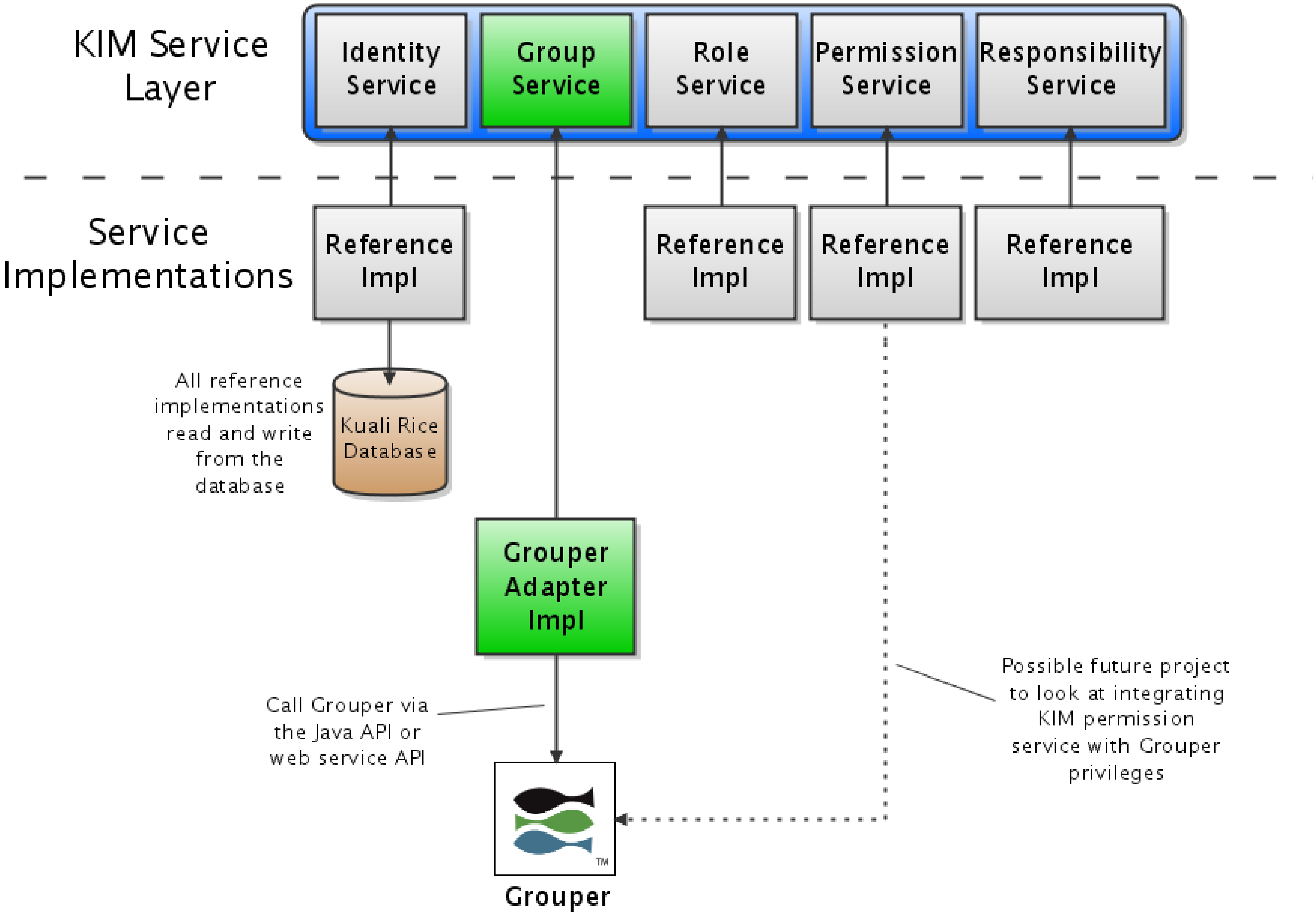
Kuali Identity Management (KIM)

- A new module of the Kuali Rice middleware framework (http://rice.kuali.org)
- Implemented as a set of services for identity and access management
- Designed with the needs of the other Kuali applications in mind (financials, research administration and student system)
- But also meant to be general enough to be used by other applications as well

KIM slides courtesy of Eric Westfall

KIM Services

- IdentityService
  - Principals and entities
- GroupService
  - Group data, group membership checks
- PermissionService
  - Authorization checks
- RoleService
  - Role data
- ResponsibilityService
  - Resolve responsibilities for certain actions (integration point with the workflow engine)
- AuthenticationService
  - Establishes an authenticated user’s session



KIM Service Layer

Identity Service

Group Service

Role Service

Permission Service

Responsibility Service

Service Implementations

Reference Impl

Reference Impl

Reference Impl

Reference Impl

All reference implementations read and write from the database

Kuali Rice Database

Grouper Adapter Impl

Call Grouper via the Java API or web service API

Possible future project to look at integrating KIM permission service with Grouper privileges

Grouper

March 2010

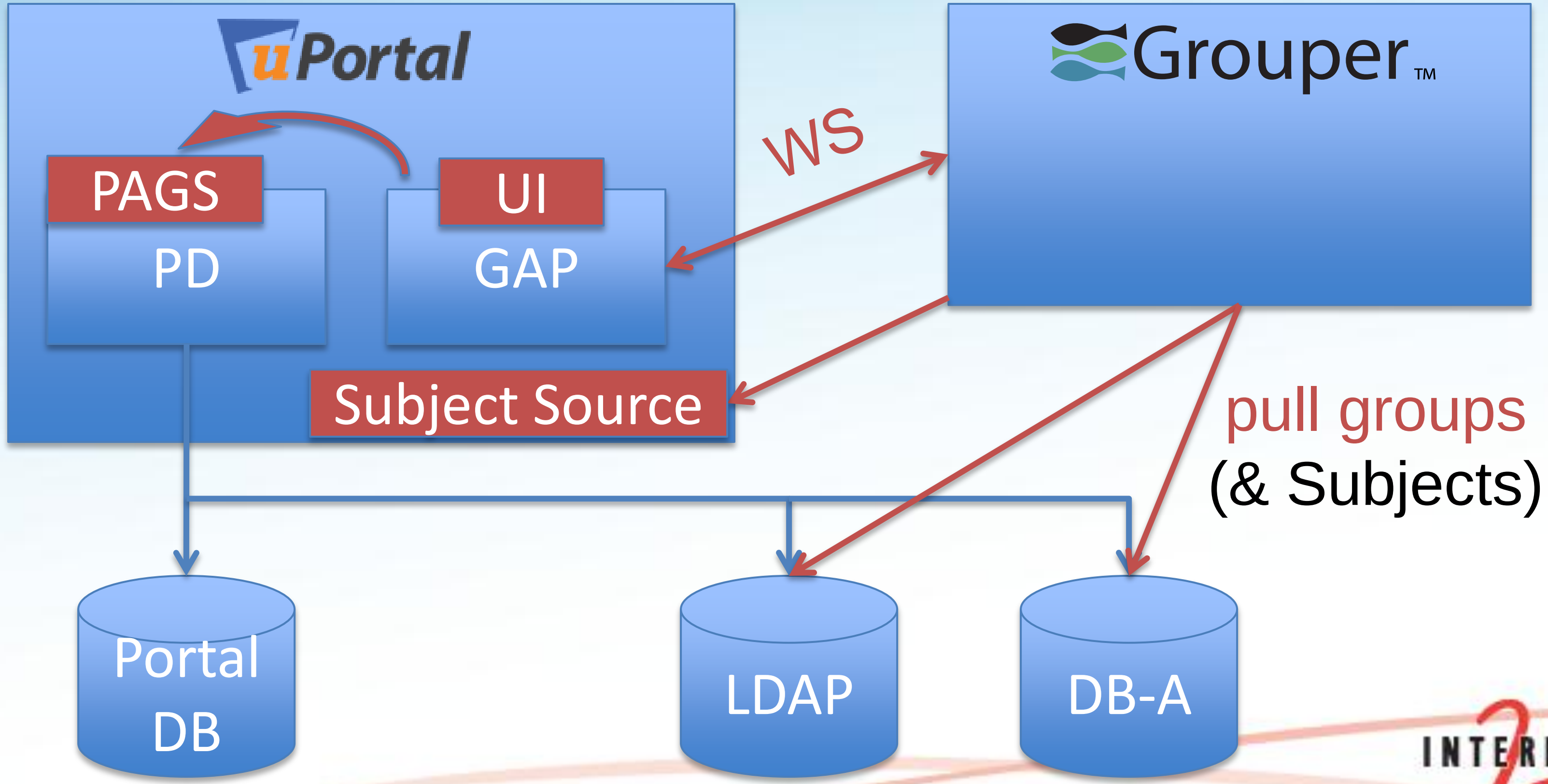
uPortal’s group-related services

- GAP: Groups And Permissions
  - Gather groups from configured group stores
  - UI to manage groups and permissions
  - Desired to outsource to Grouper
- PAGS: Person-Attribute Group Service
  - Present group memberships from attributes in user’s security context
- PD: Person Directory
  - Gather Subjects from configured stores

uPortal-Grouper integration needs

- Refactor PAGS
- New group admin UI
- Portal Subjects source adapter

- Add GAP interface
- Add group-pull



June 23-25 2010 Advance CAMP: Second Identity Services Summit

- Application developers, framework developers, campus & federated IAM infrastructure designers & implementers
- Mix of short & medium talks with unconference style collaboration
- Catalyze actual work!
- Sponsors include Internet2, InCommon, Jasig, Kuali Foundation

End matter

"The thing with integration is that it takes a lot of work, and especially in the early stages, the work has to come from the real experts, so it's expensive."

-- RL "Bob" Morgan

Advance CAMP:

https://spaces.internet2.edu/display/ACAMPIdSummit2010/Home

MACE-Paccman

https://spaces.internet2.edu/display/macepaccman/Home