

# OpenRegistry Initiative

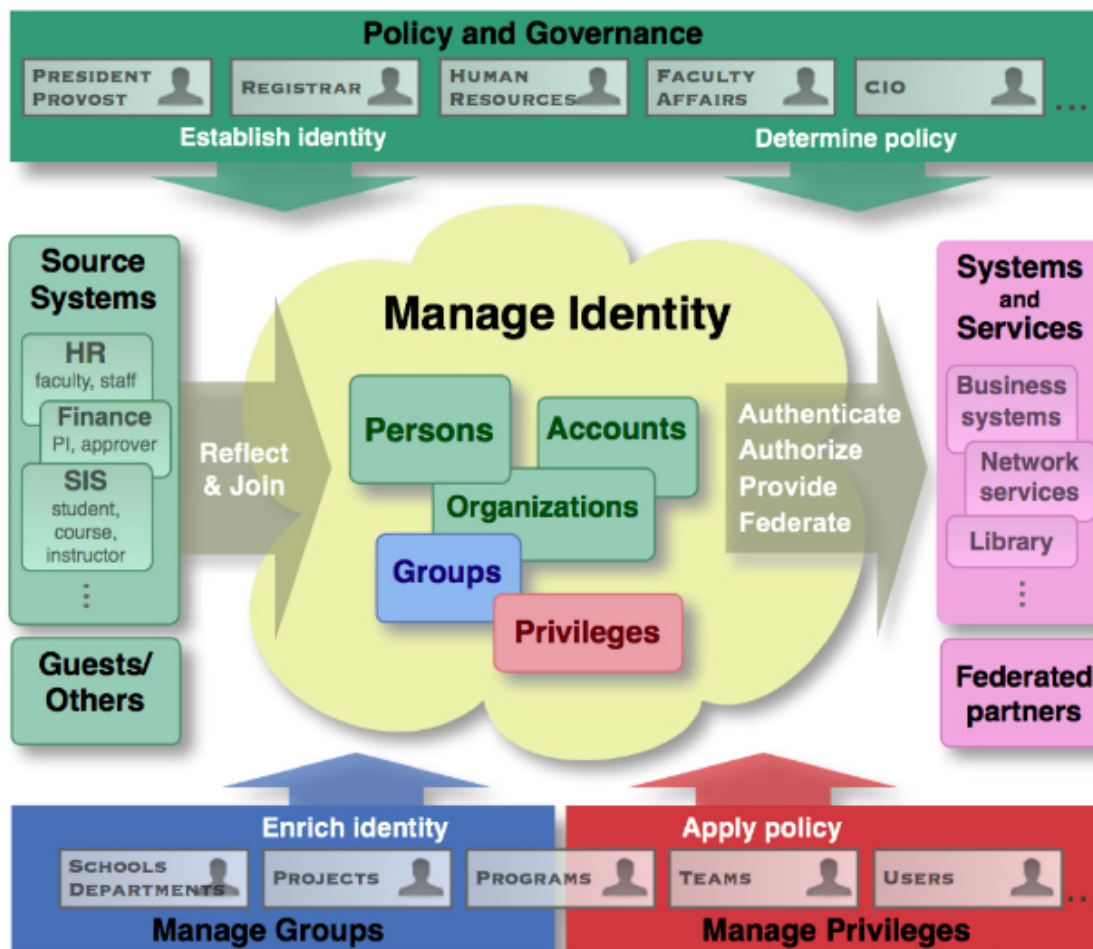
*Revisiting the Management  
of Electronic Identity*

Benjamin Oshrin  
Rutgers University  
May 2009

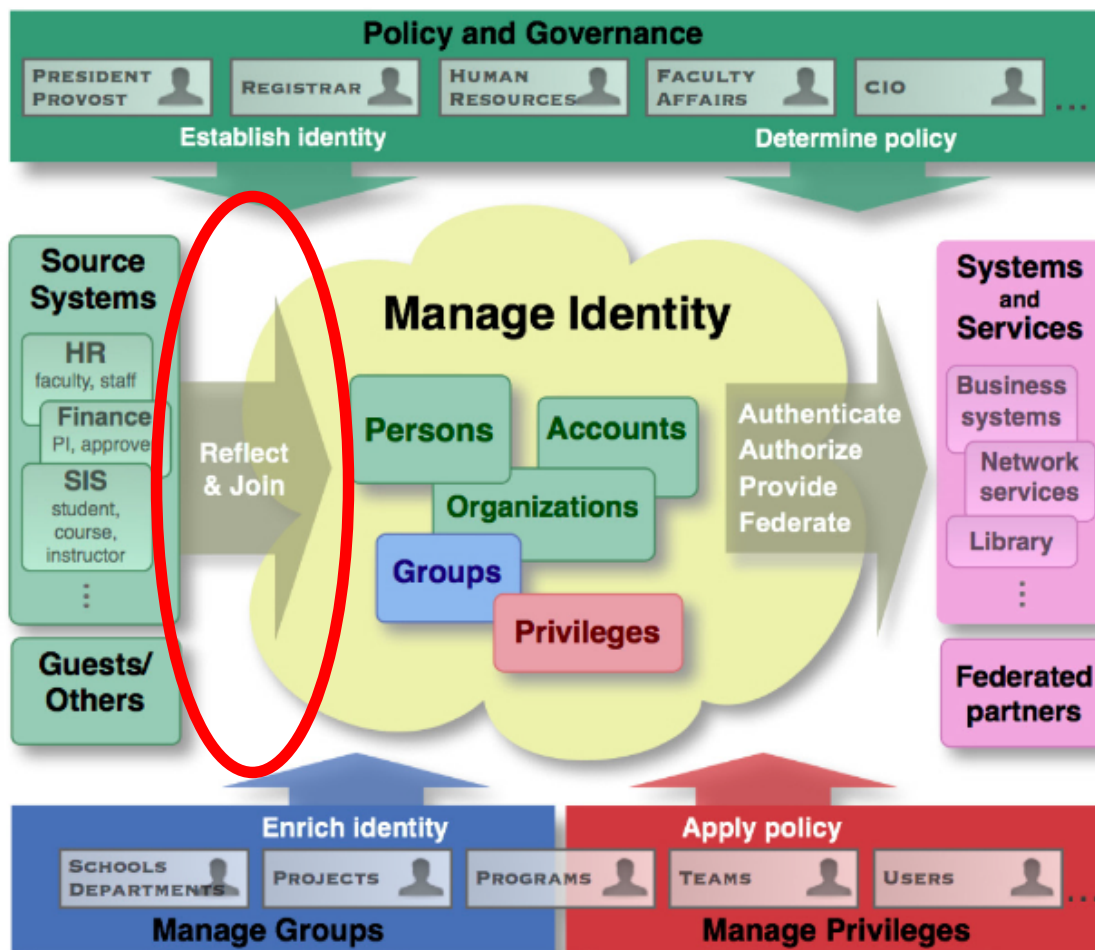
# Table of Contents

- Background
  - Identity and Access Management Models
  - What is a Registry? What is OpenRegistry?
  - Inspirations and Use Cases
- Objectives
- Approach
- Technology
  - Data Model
  - Architecture
- Milestones

# I2 Identity & Access Management Model

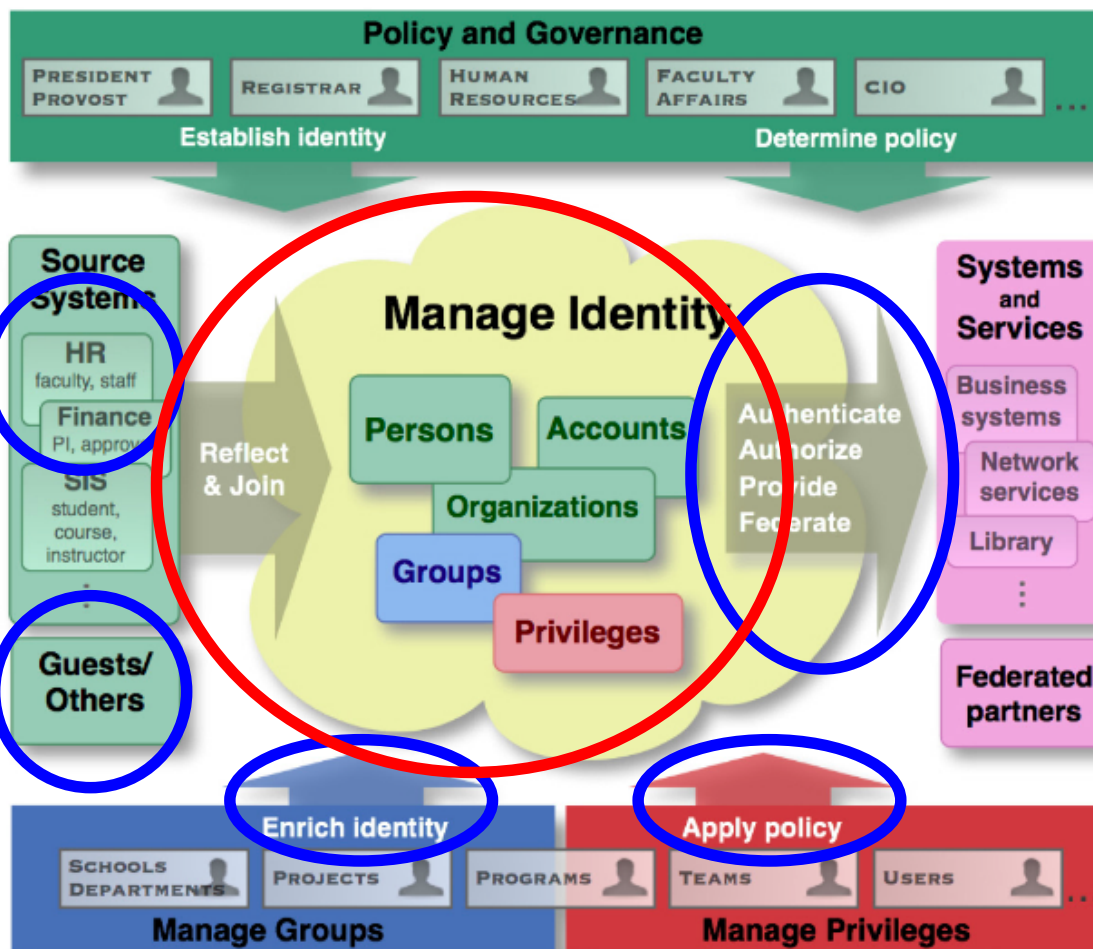


# I2 Identity & Access Management Model



OpenRegistry Core

# I2 Identity & Access Management Model



OpenRegistry Core

OpenRegistry Periphery

# What is a “Registry”?

- A definitive source of information related to a type of entity
- Person Registry: Definitive set of people affiliated with a given organization
- Other types of registries: Group, service, account, credential, course, role, business rule

# What Is OpenRegistry?

- An OpenSource Identity Management System, a place for data about people affiliated with your institution
- Core functionality
  - Interfaces for web, batch, and real-time data transfer
  - Identity data store
  - Identity reconciliation from multiple systems of record
  - Identifier assignment for new, unique individuals
- Additional functionality
  - Data beyond Persons: Groups, Courses, Credentials, Accounts
  - Business Rule based data transformations

# What Is OpenRegistry?

- More than just a Registry, some periphery too
  - Directory Builder
  - Provisioning and Deprovisioning
- Generally *not* authoritative for data
  - SORs are authoritative for most data
  - OR reflects single, reconciled view of data from multiple SORs
  - Exceptions include some identifiers, results of business rule calculations, populations with no real SOR (eg: visitors)



# Inspirations

- Columbia University Identity Management System
- Rutgers People Database
- Georgetown Model\*
- Higher Ed Standards (eg: eduPerson)
- Evolving Standards (eg: NIST LoA)
- Review of interested peer institutions
- Decades of combined experience from before the field was called “Identity Management”

# OpenRegistry @ Rutgers University

- Capture Identity Data for *all* populations affiliated with the University, including regular students, continuing ed students, joint program students, alumni, new employees, faculty, staff, retirees, and guests
  - Now: Primarily students, faculty/staff, and some “guests”
- Faster propagation of data, real time where possible
  - Now: Nightly to biweekly batch feeds
- Consistent data definitions, contracted via versions
  - Now: Hard to find definitions, unclear when they change
- Delegated operations where possible
  - Now: Heavy dependency on Help Desk and Central IT

# OpenRegistry (Select) Use Cases

- Fast identity creation for new hires (provisional hire)
- Real-time System of Record (SOR) data where SOR is capable, batch otherwise
- Guest sponsorship
- Directory construction, including real-time updates
- Provisioning/deprovisioning
- Data dictionary and versioned attribute definitions
- Password trust/levels of assurance
- ID Card integration
- Activation keys
- Roles and role specific data
- Audit history

# OpenRegistry Objectives

- Meet functional requirements of constituent institutions
- Highly scalable, highly available, modular architecture
- Easy to install, easy to configure, easy to adapt, easy to use, easy to maintain

# OpenRegistry Approach

- Communicate openly and transparently
- Design based on supportable, end-user focused, efficient processes and ease of maintenance
- Adhere to open standards wherever possible
- Leverage other higher ed efforts
- Favor iterative development where appropriate
- Implement highly available, highly scalable, cost efficient technologies

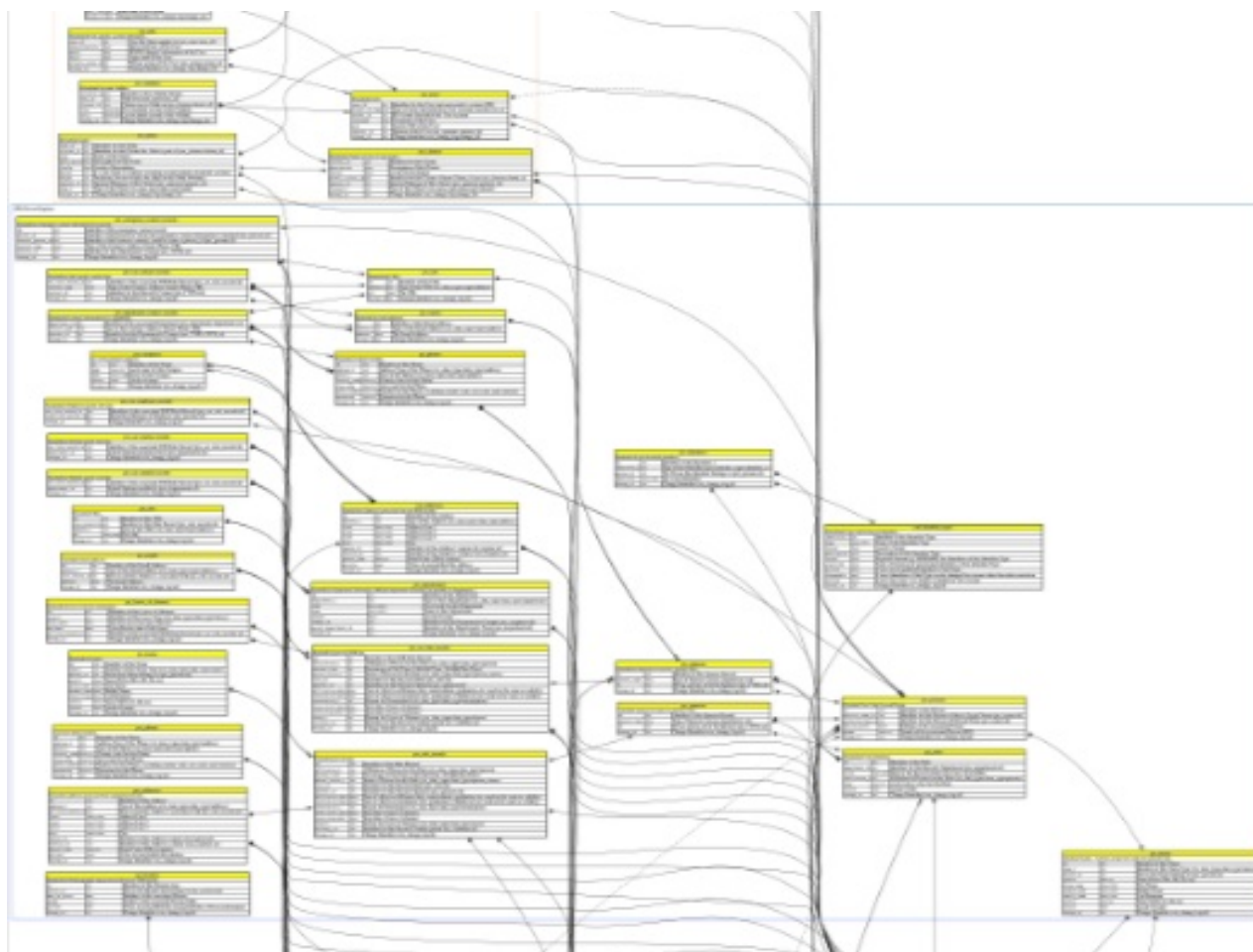
# OpenRegistry Approach

- Generic architecture and data model
  - More than Rutgers needs, but makes OR more useful for others
- Multiple levels of engagement with the community
  - Discuss: Review design documents, identify gaps and changes
  - Develop: Help write code, documentation, etc
  - Deploy: Run OR as an IDMS (when released)
  - Donate: Contribute resources to help with development and outreach
- Transparent, agile development process
  - Work done on Jasig servers, not Rutgers
- Get the ball rolling, encourage others to join
- Build on lessons learned from CAS

# Data Model

- Generic enough to work for multiple institutions
- Specific enough to work for yours
- Internationalized
- Well documented

# Data Model Overview



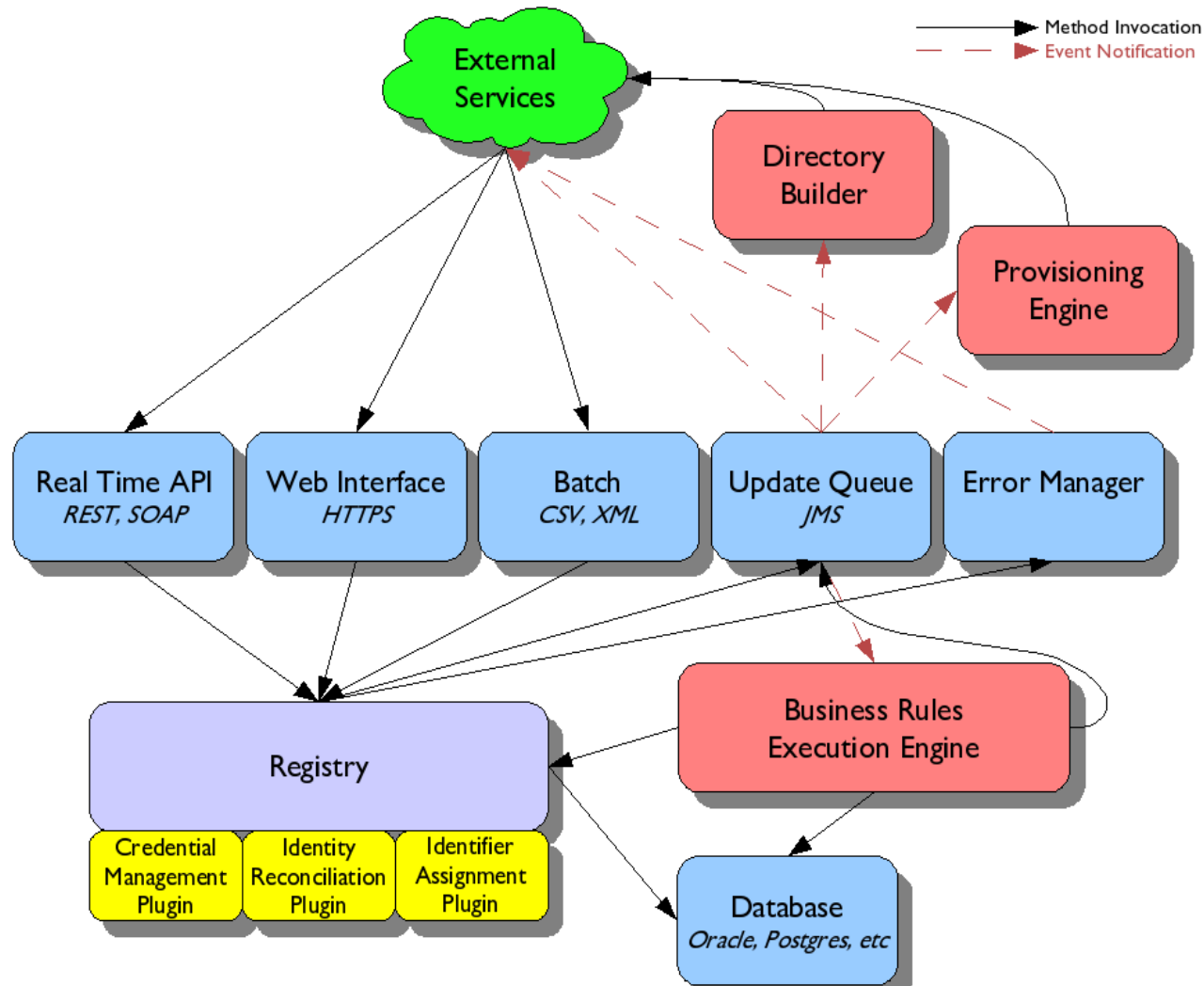


# Data Model Excerpt

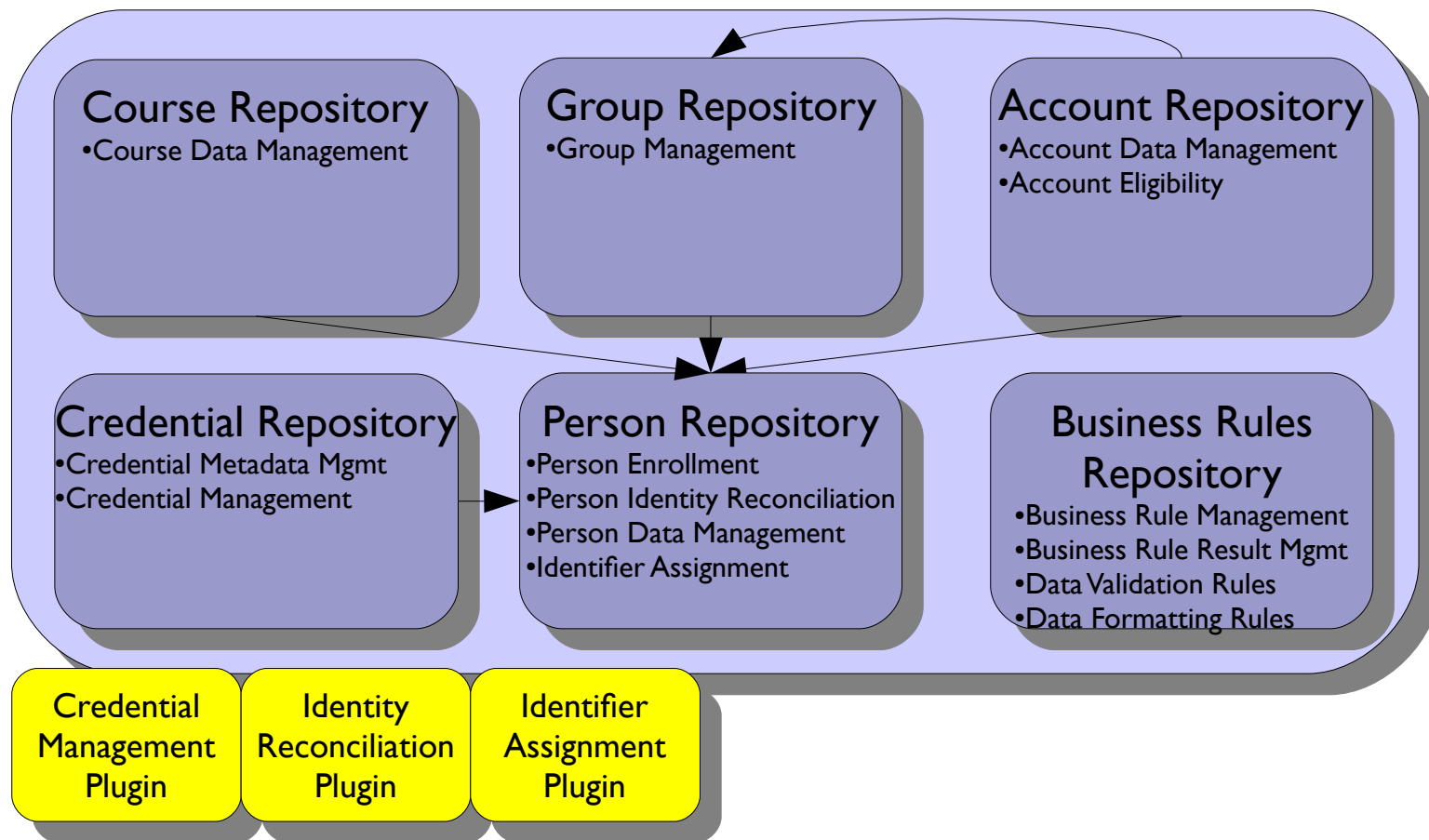
prc_affiliations		
affiliation_id	int	Identifier of this Affiliation
person_id	int	Person this Affiliation belongs to (prc_persons:person_id)
validity_id	int	Identifier for this Affiliation's Validity period (ctx_validities:validity_id)
parent_affiliation_id	int	Identifier of this Affiliation's Parent (prc_affiliations:affiliation_id)
termination_date	date	Date of effective termination (need not be same as validity)
termination_t	int	Reason for termination (ctx_data_types:data_type=termination)
affiliation_t	int	Affiliation of Person (ctx_data_types:data_type=person)
percent_time	int	Percentage of Full Time (100=Full Time, 50=Half/Part Time)
person_status_t	int	Status of Person for this Affiliation's (ctx_data_types:data_type=person_status)
role_id	int	Identifier for this Record's Affiliation's (prs_roles:role_id)
sponsor_id	int	Identifier for this Record's Sponsor (prs_sponsors:sponsor_id)
sor_role_record_id	int	Identifier of this Affiliation's SOR Role Record (prs_sor_role_records:sor_role_record_id)
change_id	int	Change Identifier (ctx_change_log:change_id)

prs_sor_employee_records		
sor_role_record_id	int	Identifier of the associated SOR Role Record (prs_sor_role_records:sor_role_record_id)
supervisor_person_id	int	Reporting Manager of Employee (prc_persons:person_id)
hire_date	date	Date of effective hire (need not be same as validity)
termination_date	date	Date of effective termination (need not be same as validity)
termination_t	int	Reason for Termination (ctx_data_types:data_type=termination)
change_id	int	Change Identifier (ctx_change_log:change_id)

# Component Architecture



# Component Architecture



[Identity Management](#)

## OpenRegistry @ rutgers.edu

Welcome, Jane Smith, administrator for Mathematics and Physics. ([Logout](#)).

### Manage Identity Data For Your Department

- ▶ [View, Add, Update, and Remove People](#)
- ▶ [Reset a Password](#)

### Manage Your Own Identity Data

- ▶ [Manage Your NetID](#)
- ▶ [Update Your Contact Information](#)
- ▶ [Manage Your Groups](#)

---

For questions or comments about this site, [contact us](#)

© 2008 Rutgers, The State University of New Jersey. All rights reserved. Last modified: 09/25/2008

[Identity Management](#)

## OpenRegistry: Your Department

Welcome, Jane Smith, administrator for Mathematics and Physics. ([Logout](#)).

### Manage Identity Data For Your Department

- ▶ [Add a New Person](#)
- ▶ View more details or update a Person (including provisional termination) by clicking on the appropriate record
- ▶ Delete a Person by checking the box in the 'Delete' column, then clicking 'Delete Selected Entries', below

NetID	Name	Title	Affiliation	Department	Good From	Good Until	Delete?
aa12	<a href="#">Alex Alexander</a>	Professor of Addition	Faculty (Provisional)	Mathematics	10/1/2008	10/31/2008	<input type="checkbox"/>
bb34	<a href="#">Beth Bethlehem</a>	Professor of Invisible Particles	Faculty	Physics	8/1/1994		<input type="checkbox"/>
cc56	<a href="#">Charles Charleston</a>	Guest Lecturer of Multiplication	Visiting Scholar	Mathematics	8/15/2007	12/31/2007	<input type="checkbox"/>

[Delete Selected Entries](#)

For questions or comments about this site, [contact us](#)  
 © 2008 Rutgers, The State University of New Jersey. All rights reserved. Last modified: 09/25/2008

[Identity Management](#)

## OpenRegistry: Add a Person

Welcome, Jane Smith, administrator for Mathematics and Physics. ([Logout](#)).

### Step 1: Personal Information

Please enter as much information as possible to help us determine if we already know about this person.

First Name*	<input type="text"/>
Middle Name	<input type="text"/>
Last Name*	<input type="text"/>
Suffix	<input type="text"/>
Date of Birth*	<input type="text"/>
NetID	<input type="text"/>
SSN	<input type="text"/>

\*Required

[Continue](#)

---

For questions or comments about this site, [contact us](#)

© 2008 Rutgers, The State University of New Jersey. All rights reserved. Last modified: 09/25/2008

[Identity Management](#)

## OpenRegistry: Add a Person

Welcome, Jane Smith, administrator for Mathematics and Physics. ([Logout](#)).

### Step 2: Possible Matches

We have found the following people who may be the person you are trying to add.

- ▶ View more details for a Person by clicking on the appropriate record
- ▶ If one of these records matches the person you are trying to add, click 'Add This Person' for that record
- ▶ If none of these records match, select 'Add New Person', below

NetID	Name	Title	Affiliation	Department	Good From	Good Until	Add?
jas12	<a href="#">John Adam Smith</a>	Administrative Assistant	Staff	English	6/15/2004		<input type="button" value="Add This Person"/>
jas34	<a href="#">John Alex Smith</a>	Unit Computing Manager	Staff	Athletics	6/15/2004	5/30/2006	<input type="button" value="Add This Person"/>

[Add New Person](#)

For questions or comments about this site, [contact us](#)

© 2008 Rutgers, The State University of New Jersey. All rights reserved. Last modified: 09/25/2008






[Identity Management](#)

## OpenRegistry: Add a Person

Welcome, Jane Smith, administrator for Mathematics and Physics. ([Logout](#)).

### Step 3: Role Information

Please enter information specific to the role your are adding.

Title	<input type="text"/>
Department	Mathematics 
Affiliation	Faculty (Provisional Type 1) 
Campus	Camden 
Good From	<input type="text"/>
Good Until	<input type="text"/>
Hide in Directory	<input type="checkbox"/>

[Continue](#)

---

For questions or comments about this site, [contact us](#)

© 2008 Rutgers, The State University of New Jersey. All rights reserved. Last modified: 09/25/2008



[Identity Management](#)

## OpenRegistry: Add a Person

Welcome, Jane Smith, administrator for Mathematics and Physics. ([Logout](#)).

### Step 4: Identity Activation

John Aron Smith has been successfully added.

- ▶ Please print this page and hand it to John for NetID activation purposes
- ▶ The address for activation of NetIDs is <https://netid.rutgers.edu/activate>
- ▶ The activation key listed below may only be used once

<b>NetID</b>	jas97
<b>Activation Key</b>	b734ff334a

[Add Another Person](#)

[Return](#)

---

For questions or comments about this site, [contact us](#)

© 2008 Rutgers, The State University of New Jersey. All rights reserved. Last modified: 09/25/2008

# OpenRegistry Initiative Milestones

- ✓ Requirements
- ✓ Design
- ✓ Project Infrastructure
- **R1: Core Services, REST API, Initial UI, Initial Business Rules**
  - Meets Rutgers RIAR-1 requirements
- R2: Enhanced Core Services, UI, Business Rules, Initial Provisioning
- R3: Batch Interface, Enhanced Business Rules, Enhanced Provisioning

# Intersection With Your Institution

- Potential for collaboration could take many forms
  - Participation in or vetting of OR design
    - Web Interface and Data Model design underway now
  - Evaluation for migration and adoption as OR matures
  - Adjustment of OR milestones according to your needs, with your resources
- Benefits of Migration to OR
  - Provides long term, sustainable model
  - Elimination of programmer-specific knowledge concerns
  - Avoidance of vendor lock-in
    - Commercial solutions aren't drop-in, customization work needed
    - Easier to tailor to future needs
  - Community of similar institutions in similar situations

## Additional Information

- <http://www.ja-sig.org/wiki/display/OR>