Rutgers Identity Attribute Registry Initiative

Revisiting the Rutgers Electronic Identity

OIT Identity Management
June 2009
Table of Contents

• Background
• Objectives
• Approach
• OpenRegistry
• Milestones
Background: ESS IDM Assessment

- 2006 effort to assess identity management services offered by OIT
- 69 page document of current deployments, emerging needs, and capability shortfalls
- Concluded that “Rutgers possesses basic identity management capabilities, though individual components are not tightly integrated. Capabilities may not be consistent, and are fractured across different projects”
Assessment: Key Findings

- Naming & Identification
  - NetIDs containing popular first/last names are increasingly difficult to obtain (less than 28% of checks for availability of a NetID are successful)
Assessment: Key Findings

• Identity Lifecycle
  – Overloading existing systems to acquire identity information makes supporting some tasks difficult (e.g. early provisioning for employees)
  – Rutgers maintains separate identity stores organized by relationship with the University. Each identity store may contain conflicting or incomplete information (which is later reconciled)
  – Individuals not easily classifiable as employees or students are not well supported. This is especially true of “casually affiliated” individuals (turf school, PALS, research collaborations) requiring limited access, for whom the existing guest process introduces excessive overhead.
  – Interpretation of attributes (e.g. student status) may differ across systems
Assessment: Key Findings

• Identity Lifecycle (ctd)
  - Lack of Standards: Point-to-point agreements typically govern terminology, data formats, or processes for transferring identity data
  - Timing Issues: Authoritative, real-time data is difficult to access outside the mainframe environment, especially from the web.
  - The reliance on batch processing results in long waits for identity creation or updates (particularly for employees).
  - Changes must be made to source (mainframe) systems are not immediately reflected in all systems. Some changes are applied to multiple databases (e.g. SRDB & PDB) to speed propagation
Assessment: Key Findings

- Directories & Registries
  - Lack of clear separation of concerns and responsibilities blurs boundaries between registry and directory data
  - Groups and Services are not well supported by the identity infrastructure
  - Direct access by consumers to underlying schema in PDB and mainframe data structures makes evolving data schemas difficult
  - Many applications do not use registries or directories directly, relying on exports of data from the PDB, Payroll, or SRDB
Assessment: Key Findings

• Authorization
  – Authorization is inconsistently implemented and applied throughout the university on an application-by-application basis.
  – Authorization data is not consistently maintained across services to reflect changes in status, access, etc.
  – Application-specific authorization data may be “orphaned” exposing future security risks should a user regain access
  – Authorization is often performed through examination of personal data or attributes, as opposed to by higher level role or group based constructs
  – Groups and roles may exist within applications, but are typically not consistent or shared between applications
Assessment: Potential Initiatives

• Non-Student/Employee Credentials
  – Develop a central system to authenticate users who do not fall into traditional student or employee categories

• Streamlined Early Identity Creation
  – Streamline and promote processes for supporting early entry of user identity data into the PDB to enable account creation, particularly for new employees

• Person Registry
  – Create a person registry centralizing core data for creating, linking, and reconciling digital identities

• Real-time Identity Data
  – Provide real-time access to authoritative identity data
Assessment: Potential Initiatives

- Enterprise Group Service
  - Provide a centralized grouping service supporting automatically generated and ad-hoc groups

- Enterprise Authorization Model
  - Perform a detailed survey of current authorization requirements and approaches to develop a standard model for authorization for ESS service

- Various additional initiatives also identified
  - Automated Provisioning
  - Levels of Assurance
  - RUConnection Integration
  - [Your personal favorite here]
Background: People Database (PDB)

- “A single source record for each student, faculty and staff with associated information (i.e. roles, campus address)” (1999)
- Provides directory-like and registry-like non-authoritative access to personal information copied from authoritative systems (payroll, SRDB) including emergency contact information, disclosure information, personal URL, email; roles within the University, and multiple addresses and phone numbers aggregated from the authoritative data sources
- Receives data from Payroll, SRDB, various “guest” procedures, select other sources, but not all alumni, continuing ed students, etc
Background: People Database (PDB)

- Authoritative source for user NetIDs and publicly displayed email addresses
- Generates IID \((jqs12)\) on user entry
- Uses RCPID (private system-to-system identifier) as primary key
- Authoritative source for disclosure attributes used to indicate user privacy preferences
- Public personal information is displayed within the Rutgers online directory (subject disclosure attributes) and accessed by or fed to various applications
- Several specific web applications are also provided for privileged access to user information (e.g. Dean’s View)
Registry Initiative Objectives

- 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
- Faster propagation of data, real time where possible
- Consistent data definitions, contracted via versioning
- Delegated operations where possible
Registry Initiative Approach

- Communicate openly and transparently
- Design based on supportable, end-user focused, efficient processes
- Avoid proprietary, one-off solutions and the associated long term maintenance issues
- Adhere to open standards wherever possible
- Leverage other higher ed efforts
- Develop iteratively, avoid big-bang cutovers
- Implement highly available, highly scalable, cost efficient technologies
- Provide technology leadership
I2 Identity & Access Management Model

Policy and Governance
- President
- Provost
- Registrar
- Human Resources
- Faculty Affairs
- CIO

Establish identity
Determine policy

OpenRegistry Core

OpenRegistry Periphery

Manage Identity
- Persons
- Accounts
- Organizations
- Groups
- Privileges

Systems and Services
- Business systems
- Network services
- Library
- Federated partners

Source Systems
- HR
- Finance
- SIS
- Guests/Others

Reflect & Join

Enrich identity
Apply policy

Manage Groups
Manage Privileges

Office of Information Technology/Identity Management Group
OpenRegistry Initiative

• Rutgers Registry to be built on OpenRegistry platform, developed by Rutgers, along with other Universities

• 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

• More than just a Registry, some periphery too
  – Directory Builder
  – Provisioning and Deprovisioning
OpenRegistry IDM Technical Model

- Systems of Record
- "Ad Hoc" Sources
- Identity Reconciliation
- Identity Business Rule Execution
- Person Registry
- Identity Service Provisioning
- Identity Reporting Database

Sources

<table>
<thead>
<tr>
<th>Sources</th>
<th>Internal Processes</th>
<th>External Services</th>
<th>Consumers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Applications</td>
<td>Server Logins</td>
<td>Desktop Logins</td>
<td>Data Managers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Auditors</td>
</tr>
</tbody>
</table>

Office of Information Technology/Identity Management Group
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 (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
Data Model

- Generic enough to work for multiple institutions
- Specific enough to work for ours
- Internationalized
- Well documented
Data Model Overview
# Data Model Excerpt

### prc_affiliations

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

### prs_sor_employee_records

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sor_role_record_id</td>
<td>int</td>
<td>Identifier of the associated SOR Role Record (prs_sor_role_records:sor_role_record_id)</td>
</tr>
<tr>
<td>supervisor_person_id</td>
<td>int</td>
<td>Reporting Manager of Employee (prc_persons:person_id)</td>
</tr>
<tr>
<td>hire_date</td>
<td>date</td>
<td>Date of effective hire (need not be same as validity)</td>
</tr>
<tr>
<td>termination_date</td>
<td>date</td>
<td>Date of effective termination (need not be same as validity)</td>
</tr>
<tr>
<td>termination_t</td>
<td>int</td>
<td>Reason for Termination (ctx_data_types: data_type=termination)</td>
</tr>
<tr>
<td>change_id</td>
<td>int</td>
<td>Change Identifier (ctx_change_log:change_id)</td>
</tr>
</tbody>
</table>
Component Architecture
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
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

<table>
<thead>
<tr>
<th>NetID</th>
<th>Name</th>
<th>Title</th>
<th>Affiliation</th>
<th>Department</th>
<th>Good From</th>
<th>Good Until</th>
<th>Delete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>aa12</td>
<td>Alex Alexander</td>
<td>Professor of Addition</td>
<td>Faculty (Provisional)</td>
<td>Mathematics</td>
<td>10/1/2008</td>
<td>10/31/2008</td>
<td>✔️</td>
</tr>
<tr>
<td>bb34</td>
<td>Beth Bethlehem</td>
<td>Professor of Invisible Particles</td>
<td>Faculty</td>
<td>Physics</td>
<td>8/1/1994</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
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.

<table>
<thead>
<tr>
<th><strong>First Name</strong>*</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Middle Name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Last Name</strong>*</td>
<td></td>
</tr>
<tr>
<td><strong>Suffix</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Date of Birth</strong>*</td>
<td></td>
</tr>
<tr>
<td><strong>NetID</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SSN</strong></td>
<td></td>
</tr>
</tbody>
</table>

*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
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

<table>
<thead>
<tr>
<th>NetID</th>
<th>Name</th>
<th>Title</th>
<th>Affiliation</th>
<th>Department</th>
<th>Good From</th>
<th>Good Until</th>
<th>Add?</th>
</tr>
</thead>
<tbody>
<tr>
<td>jas12</td>
<td>John Adam Smith</td>
<td>Administrative Assistant</td>
<td>Staff</td>
<td>English</td>
<td>6/15/2004</td>
<td></td>
<td>Add This Person</td>
</tr>
<tr>
<td>jas34</td>
<td>John Alex Smith</td>
<td>Unit Computing Manager</td>
<td>Staff</td>
<td>Athletics</td>
<td>6/15/2004</td>
<td>5/30/2006</td>
<td>Add This Person</td>
</tr>
</tbody>
</table>

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
OpenRegistry: Add a Person

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

**Step 3: Role Information**

Please enter information specific to the role you are adding.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Department</td>
<td>Mathematics</td>
</tr>
<tr>
<td>Affiliation</td>
<td>Faculty (Provisional Type 1)</td>
</tr>
<tr>
<td>Campus</td>
<td>Camden</td>
</tr>
<tr>
<td>Good From</td>
<td></td>
</tr>
<tr>
<td>Good Until</td>
<td></td>
</tr>
<tr>
<td>Hide in Directory</td>
<td></td>
</tr>
</tbody>
</table>

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
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

<table>
<thead>
<tr>
<th>NetID</th>
<th>jas97</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Key</td>
<td>b734ff334a</td>
</tr>
</tbody>
</table>

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
Registry Initiative Milestones

Rutgers Registry Initiative

- RIAR-1: DCEO Students
  - Callouts to and data synchronization with PDB
  - Built on OpenRegistry R1
- RIAR-2: ID Card Integration
  - Provisional privileges until SOR data is processed
- RIAR-3: SOR Data
  - Process SOR data (HR, Student, and possibly others) directly
- RIAR-4: TBD
- ...

OpenRegistry Initiative

- R1M1: Requirements
- R1M2: Design
- R1M3: Project Infrastructure
- R1M4: Project Services
- R1: First Production Functionality
  - Meets RIAR-1 requirements
Additional Information

• http://idms.rutgers.edu/registry
• http://idms.rutgers.edu/contact
• http://www.ja-sig.org/wiki/display/OR