Registries and Records: The Ties That Bind an IAM System

IAM Online
February 17, 2016 – 2 pm ET

Warren Curry, IAM Architect, University of Florida
Chuck Moore, Business Relationship Manager, Penn State
Renee Shuey, Senior Director, Identity Services, Penn State
What is a Central Person Registry?

• A single, authoritative source for all person identity information
• A hub for enabling distributed management of identity information
• A real-time transaction engine for this information
Why have a Central Person Registry?

- Ensure high-quality person identity information in a single data storage location
- Reduce and eliminate duplicate IDs
- Provide transparent, auditable, verifiable business rules
- Provide service management and governance
- Self-service interfaces for individuals and administrative units
- Interfaces for requests for service, notifications, access approval, and managing identity data
The Identity and Access Management Project and the CPR

- In 2008, the IAM project was created to develop a roadmap for Identity Management at Penn State
- The proposal was delivered to Kevin Morooney, CIO
The IAM Report: Recommendations

1. Create a comprehensive policy for IAM
2. Develop a plan for formal risk assessment
3. Create a central person registry
4. Add Level of assurance to access decisions
5. Promote better control of digital credentials
6. Streamline vetting, proofing and issuance of credentials
7. Automate provisioning/deprovisioning of access rights
8. Promote awareness and education of IAM
The Identity and Access Management Project and the CPR

• 2008 – IAM Technical Architect Group (TAG) formed to implement recommendations
• 2008-2012 – IAM TAG builds CPR
• 2013 Identity Services department formed to put CPR into production, deliver on roadmap
• Summer, 2013 – CPR enters Production
What Types of Data?

- Biographical information (names, addresses, email addresses, telephone numbers, gender, and date of birth)
- ID Card information (including photo)
- Person and account linkages
- Directory confidentiality preferences
- Digital credential information (support exists for multiple credentials per person)
- Identity assurance information to include the event history
- Internal and external affiliation support
Who is Using the CPR?

• Customers include
  • Student Information System
  • HR Information System
  • Police Services
  • Library
  • Office of the Bursar
  • Finance and Business Services
  • Admissions
  • World Campus
Trust and Relationships

• The new environment
  • Overcoming silos
  • Building trust
  • Data sharing
  • Shared decision making
One Record To Rule Them All

• Which record is ‘primary’?
• Which record is ‘correct’?
• How do we keep the systems in sync?
Administrative Policy Addresses Identity

• In October 2014, Penn State implemented Policy AD80 – Identity and Access Management
  • Designated the CPR as the authoritative source for identity information
  • Defined Identity Authorities as “business units authorized by IAM Governance with the responsibility to create or update identities in the CPR”
  • Called for ongoing governance to approve the strategic direction of identity and access management
Person Biographical (Bio) Record

• In order to simplify compliance with policies and procedures related to AD80, Identity Services and the Enterprise Project Management Office convened a new working group

• The group, consisting of stakeholders from across Penn State, developed the Person Biographical Record
Person Biographical (Bio) Record

• A shared set of core and non-core data elements containing information related to person identity
• Stored in data fields whose definitions are collectively understood and adhered to
• Created and maintained under shared policies and procedures
• A high degree of consistency, confidence, and data integrity for identity information across Penn State information systems
Person Biographical (Bio) Record
Minimum Data Fields

• Required at the time of record creation
  • Name
  • Date of Birth
  • Gender
  • Address
Core Data Elements

• Must be requested at the time of record creation
  • Taxpayer Identification Number (SSN)
  • Email Address
Non-Core Data Elements

• Become part of the Person Bio Record if they are collected
  • Phone Number
  • Citizenship
  • Visa Data
  • Photo
Person Bio Record Shared Policies

- Standardized and uniform across Penn State systems, regardless of the person’s affiliations to the university or which Identity Authority is performing the transaction
- Approved entities may pull information from the Person Bio Record for use in a local system
- Only Identity Authorities can write data values to the Person Bio Record
University of Florida

Identity and Access Management and Registry
Elements of Identity and Access Management

UF IAM Governance

Policies

UF Identity Registry

Entities

Attributes

Entitlements

GatorLink

User Account Management

Credentialed

Role(s)

Rule(s)

Access Request System (ARS)
POLICY is a MUST to REGISTRY

UF Identity Management (IdM) Policy

- **PURPOSE**

  The university requires a secure and reliable method of identifying members of its community for access to electronic data resources. This requires collecting and maintaining identifying attributes, ensuring that electronic identities match the appropriate persons, and mechanisms to authenticate and authorize use of those identities.


- **The policy:**
  - Defines Scope
  - Has Policy Statements
  - Defines Responsibility
  - Has supporting Standard Documents
Identity Framework with UF detail

IAM Console
IDM – Manage Identity Information
GatorLink Account Management
Access Request System

Identity Registry
UF Registry (Master Person Data)

Access Management
ARS, AD Groups, Application specific tools

Authentication
UF AD
Shibboleth.

Provisioning & Integration
ARS, UF AD, myUFL Portal

Other IAM Components
AD/LDAP/BizTalk/Integration Broker
Registry API’s, GDRC ODS

Target Systems
HR, UF Health HR, DCE, Student Records

Systems of Record For Automated Affiliations
HR, UF Health HR, DCE, Student Records
Registry – A Component of the Larger IAM Ecosystem

- **Source of Person Data**
  - Feeds systems of record
  - Each Person gets a UFID
  - HR, SIS, DCE use person data from registry.
  - HR, SIS DCE feed affiliation info to registry
  - Person must exist in registry prior to HR, SIS, DCE

- **Departments can enter people into registry**
  - Registry Coordinator
  - Registry Administrator
  - Person is data Owner
  - Self Management encouraged
UF Identity Registry the source of "person-ness"

Registry as Data Hub

Enterprise Services Bus

AD DS

Kerberos

API

Registry

OneIT for the #GatorGood
Registry – an Entity Registry

- **Person**
  - 2.2 million in UF Registry
    - Small number of duplicates
    - Matching issues are reduced in HUB
    - Real/near-time updates

- **Guest (7 day/ lightweight/ limited)**

- **Organizations**
  - Issued UFID like person

- **More support needed for:**
  - Service and Privileged Identities
  - Things On the Internet
Registry – an Entity Registry

- If you need to define as a member of a group
- If it requires access privileges
- If it is a person of ongoing interest
- If it is an organization group
- Affiliation is relationship - Person to Organization
- Person to Person (household)
- Person to University Role (President, Dean, etc)
- Do not overdue groups in the registry: better tools exist for this… (Grouper, for example)
UF Identity Registry

DB2

Persons
Organizations
Relationship Types
Identifiers
Person Attributes
Affiliations
Person to Organization
IT Relationship
Person to IT Unit
Personal Relationships
Person to Person
Role Relationship
Person to Role

Registry Transactions

Maintain API’s
Obtain API’s
Browse API’s
Views to DB

Java/APIs
Direct/APIs
Direct/APIs

Management User Interface
Gator Link

Other Consuming Systems

OneIT for the #GatorGood
Registry – an Entity Registry

- Store person info: source
- Store identifiers for the person
- Associate to computer access credential
- Store the data that belongs to the person
  - Name(s)
  - Email, Phone, Addresses, etc.
  - Attributes of person unaffected by any business system
  - Reflects and transforms SOR data to serviceable values for Federation
- Events drive info to Target systems.
- Contains info for EduPerson attributes
Began in early 1990s – simple flat data

1996 – 2003 had 18 Sources being pushed to a single sink
  ◦ Duplicates a big issue
  ◦ Which input contained “correct” info for person
  ◦ Data Currency of Source and update frequency of source

2003 – 2009
  ◦ Data hub quality of data increased very much
  ◦ Event message queues
  ◦ Source of person info

2008 - 2016
  ◦ Messaging
  ◦ Expanded Attributes and Release Policy

2016 – forward
  ◦ Master data infrastructure
  ◦ API Gateway added to messaging
  ◦ Data Trustee who is not IT centric / UF wide governance
  ◦ Data model tweaks
  ◦ TIER and more federation readiness
TIER Registry Workgroup

- Newly formed group to assist TIER project with Registry requirements
- Reviewing several sets of requirements
- Use cases and features from multiple sources
- Prepare initial deliverable to TIER project April 2016
- Phone calls on Wednesday afternoons or Friday mornings. Working closely with API and data workgroup

- [https://spaces.internet2.edu/display/TWGH/TIER+Working+Groups+Home](https://spaces.internet2.edu/display/TWGH/TIER+Working+Groups+Home)
Questions
IAM Online Evaluation

Please complete a short evaluation of today’s presentation

InCommon Shibboleth Installation Workshops

May 19 - 20, 2016 – University of Chicago
Two more to be scheduled in the first half of 2016

Details and registration at incommon.org/shibtraining