Registries

Scott Koranda

November 2018

Zanzibar

The Leonard E. Parker
Center for Gravitation, Cosmology & Astrophysics
at the University of Wisconsin–Milwaukee

User Directories Registries Data Store

Scott Koranda

November 2018

Zanzibar

The Leonard E. Parker
Center for Gravitation, Cosmology & Astrophysics
at the University of Wisconsin–Milwaukee

Identity Registry

- Database for storing, curating, and managing electronic identities for people
- Usually for the purpose of managing access to electronic services
- People details shared with “downstream” services often determined or at least managed by Registry

No Universal Incumbent

- For many years each university wrote its own registry to satisfy its own local use cases
- Many universities still do...

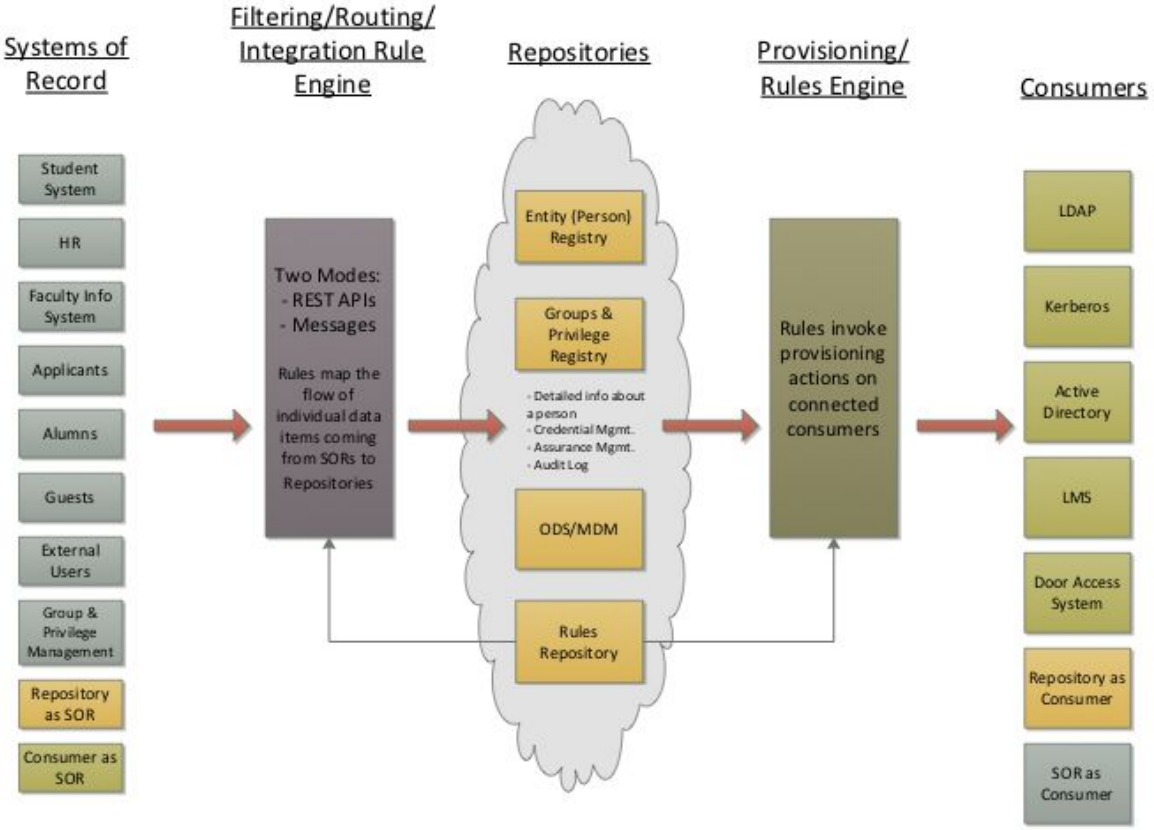
No Universal Incumbent

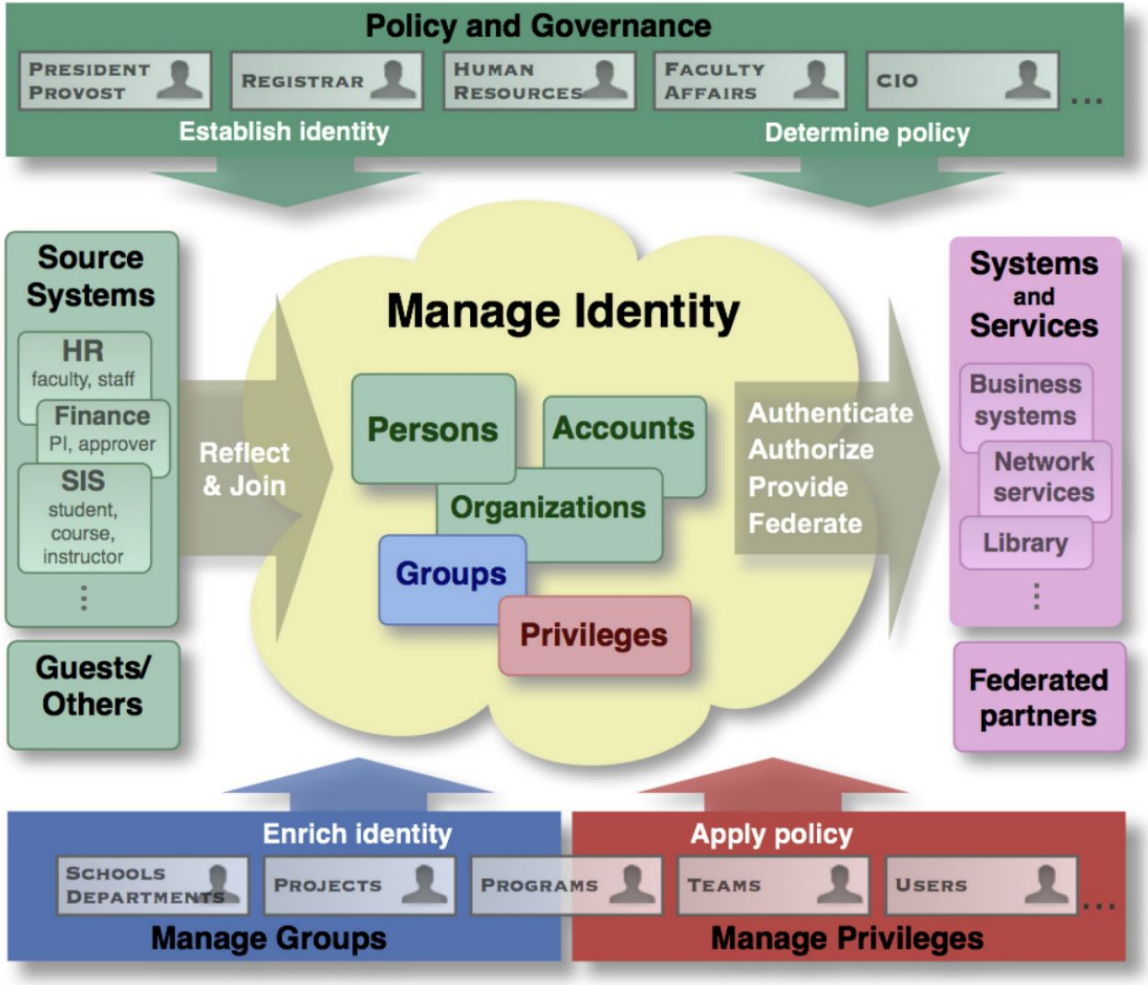
- More recently some universities working together to create a “Registry for Higher Education and Research” (with mixed success)
- Newer enterprise and open source efforts aimed at different scales of organizations

Architecture

Where does the Registry sit in an Identity and Access Management (IAM) architecture?

Identity Ecosystem




Policy and Governance
President
Provost
Registrar
Human Resources
Faculty Affairs
CIO
...
Establish identity
Determine policy
Source Systems
HR
faculty, staff
Finance
PI, approver
SIS
student, course, instructor
Guests/ Others
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
Manage Groups
Apply policy
Teams
Users
Manage Privileges

Focus on Capabilities

What capabilities should you consider as you select (or build) a registry for your higher education or research organization?

Onboarding

- Onboarding is how the electronic identities for people come into the registry so they can be managed
- Two general categories of onboarding
  1. Enrollment directly into the person registry
  2. Consumption from other systems of record (SOR)

Onboarding: Enrollment

- Enrollment is often initiated by a privileged user
  - e.g., someone from admissions office
  - User is asked to add identifiers and attributes
    - Name, postal address, mobile number, …
  - May prompt user to create credential (password)
  - Creates a “petition”
  - Petition may progress through different approval processes
- Call this “administrator initiated” enrollment

Onboarding: Enrollment

- “Self-signup” enrollment
  - User initiates process to create petition
  - Usually involves filling out form(s)
  - Later the petition is (usually) reviewed and winds through an approval process
  - More common with research organizations and collaborations than with higher education institutions

Enrollment Capabilities

- Flexible enrollment flows
  - Administrator, self-signup, conscription
  - Simple to complex petition approval process
- Extensible collection of identifiers and attributes
- Rich and extensible set of petition states
  - Not just “active” and “inactive”

Onboarding: ingest from SOR

- Most often registry consumes electronic identity(ies) from an external System Of Record
  - Human Resources (HR) database
  - Student Registrar database
  - Email database
  - National student registry system
- Quite often the single person registry record is constructed from multiple SOR records

Ingestion from SOR: Capabilities

- Support for ingesting from multiple SOR
- Match across multiple SOR inputs to create single registry record
- Match against existing identities in registry
- Record history
- Synchronization with SOR
  - How often?
  - Which identifiers and attributes update and how?

Strategies for Registry Success

- Respect SOR data (and its owner)
  - SOR data can be messy
  - Take it as it comes and follow Postel's law (paraphrased): "Be liberal in what you accept from others, conservative in what you pass along"
- Add value when possible to the other SOR
  - Often the data in the Identity Registry can be more refined and ultimately useful
  - Work with SOR owners to see if they can benefit from receiving data back from the Registry

Some Tools to Consider...

COmanage™

- Open Source from Internet2/InCommon in US
- Adopted by Internet2 TIER program
- "...a tool for identity enrollment and lifecycle management of people associated with your organization. Suitable for small collaborations with tens of people or large universities with hundreds of thousands...allows you to organize complex identity data from multiple sources to create a single view of a person."

midPoint

- Open Source from Evolveum
- Adopted by Internet2 TIER program
- Features of midPoint include identity governance, provisioning and audits, organization structure, entitlement management, credential management, and workflow.

WSO2 Identity Server

- Open Source from WSO2
- "WSO2 Identity Server...is a uniquely flexible, open source IAM product optimized for identity federation and SSO with comprehensive support for adaptive and strong authentication."

UWM

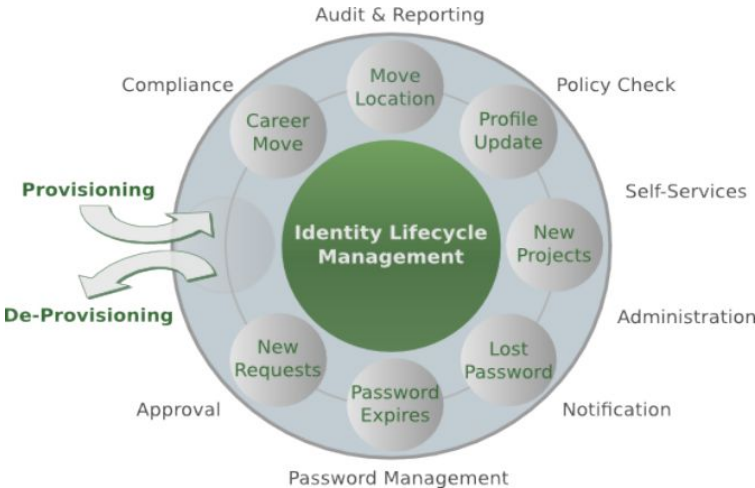
- From RedHat
- "Open Source Identity and Access Management For Modern Applications and Services"
- "Add authentication to applications and secure services with minimum fuss. No need to deal with storing users or authenticating users. It's all available out of the box. You'll even get advanced features such as User Federation, Identity Brokering and Social Login."

OpenIAM Identity Manager

- "The OpenIAM Identity Manager automates the task of managing identities across the various devices and applications used by the enterprise. This includes applications within the enterprise such as Active Directory and Exchange, and cloud based applications such as Google Apps."
- Community Edition is Open Source

Apache Syncope

- "Apache Syncope is an Open Source system for managing digital identities in enterprise environments, implemented in Java EE technology and released under Apache 2.0 license"

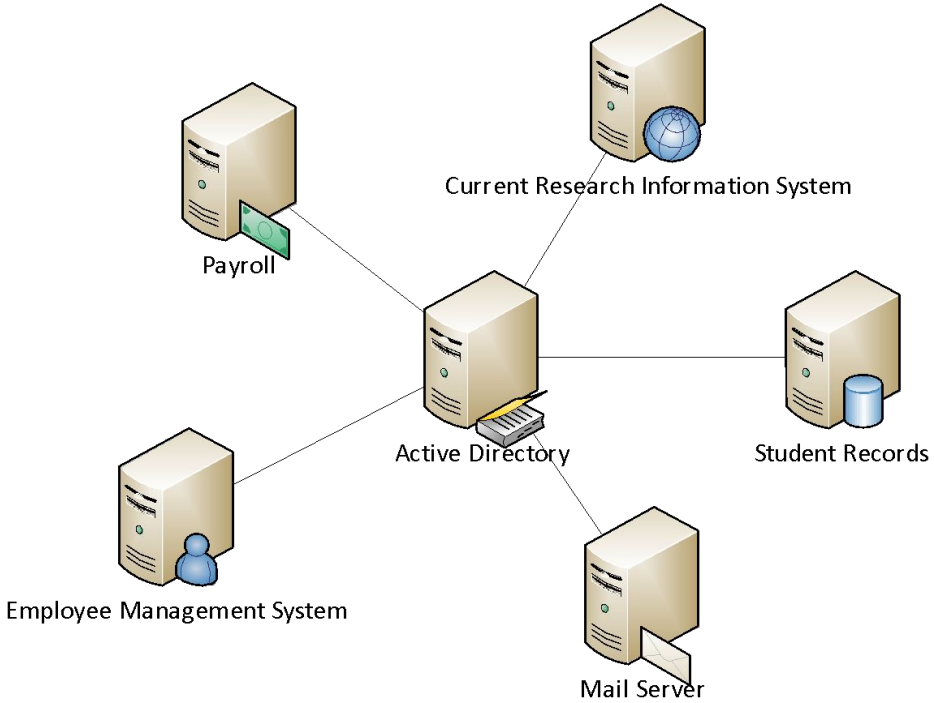


OpenAM

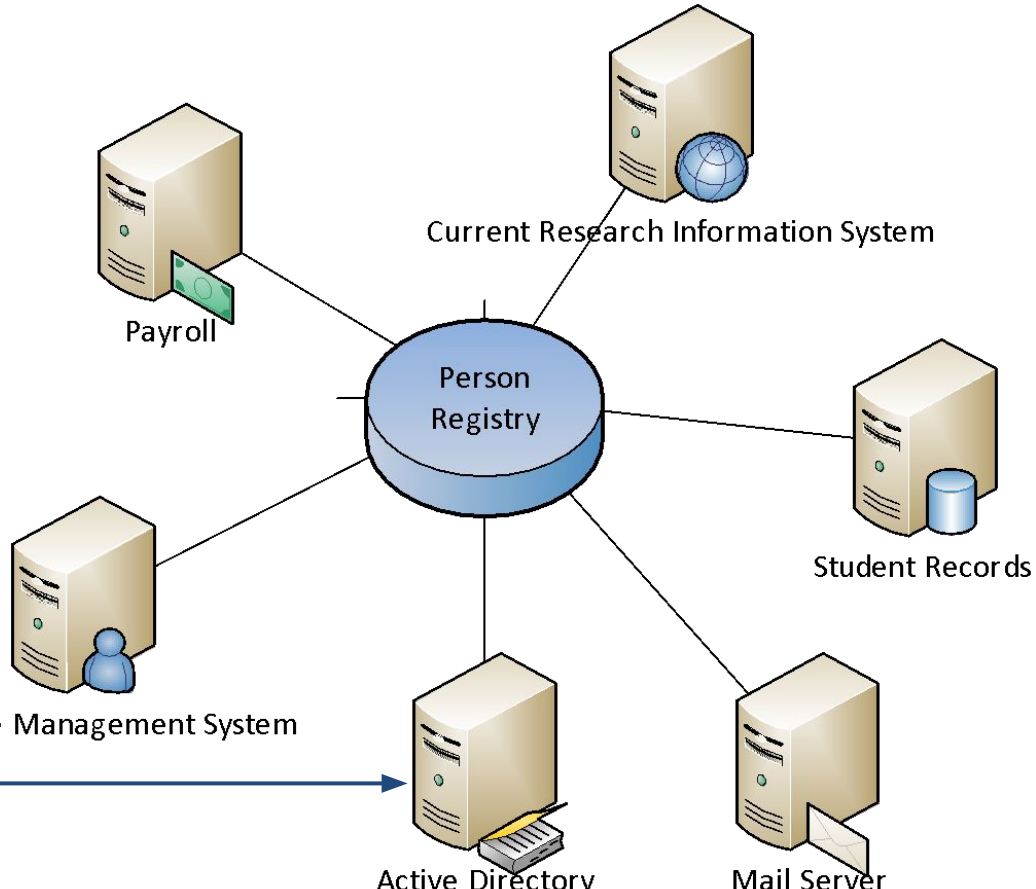
- OpenAM is an open source access management, entitlements and federation server platform
- It was sponsored by ForgeRock until 2016, now it is supported by Open Identity Platform Community
- Originated as OpenSSO by Sun Microsystems, later by Oracle Corporation.
- OpenAM is a fork which was initiated following Oracle's purchase of Sun

Microsoft AD

"Let's put everything in AD"



Microsoft AD



AD is just another consumer of Identity

Microsoft Identity Manager 2016

- "On-premises identity and access management Synchronize identities between directories, databases and apps. Administer self-service password, group and certificate management. Increase admin security with policies, privileged access and roles."

Microsoft

NetIQ (Novell) Identity Manager

- "The comprehensive solution for provisioning identities and controlling access
  Identity Manager delivers a complete, yet affordable solution to control who has access to what across your enterprise—both inside the firewall and into the cloud. It enables you to provide secure and convenient access to critical information for business users, while meeting compliance demands."

IBM Tivoli Identity Manager

- Provides centralized identity lifecycle management
- Automatically create, manage, and delete user access to various system resources such as files, servers, applications, and more based on job roles or requests

Oracle Identity Manager

- "Oracle Identity Manager is a Governance solution that provides self service, compliance, provisioning and password management services for applications residing on-premise or on the Cloud"
- "makes it possible for enterprises to manage the identities and access privileges of their customers, business partners, and employees, all on a single platform"

ForgeRock Identity Platform

- "We built the ForgeRock Identity Platform from the ground up, designed from the outset as a unified model to integrate with any of your digital services."
- "Purpose-built to seamlessly manage identities across all channels, on-premises, in the cloud, and on mobile"