Registries

Identity Management & Federation 2019

With acknowledgements to Scott Koranda

Identity Registry

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

No universal incumbent

- For many years each university wrote its own registry to satisfy its own local use cases
- Or worse, developed a set of disjoint integrations

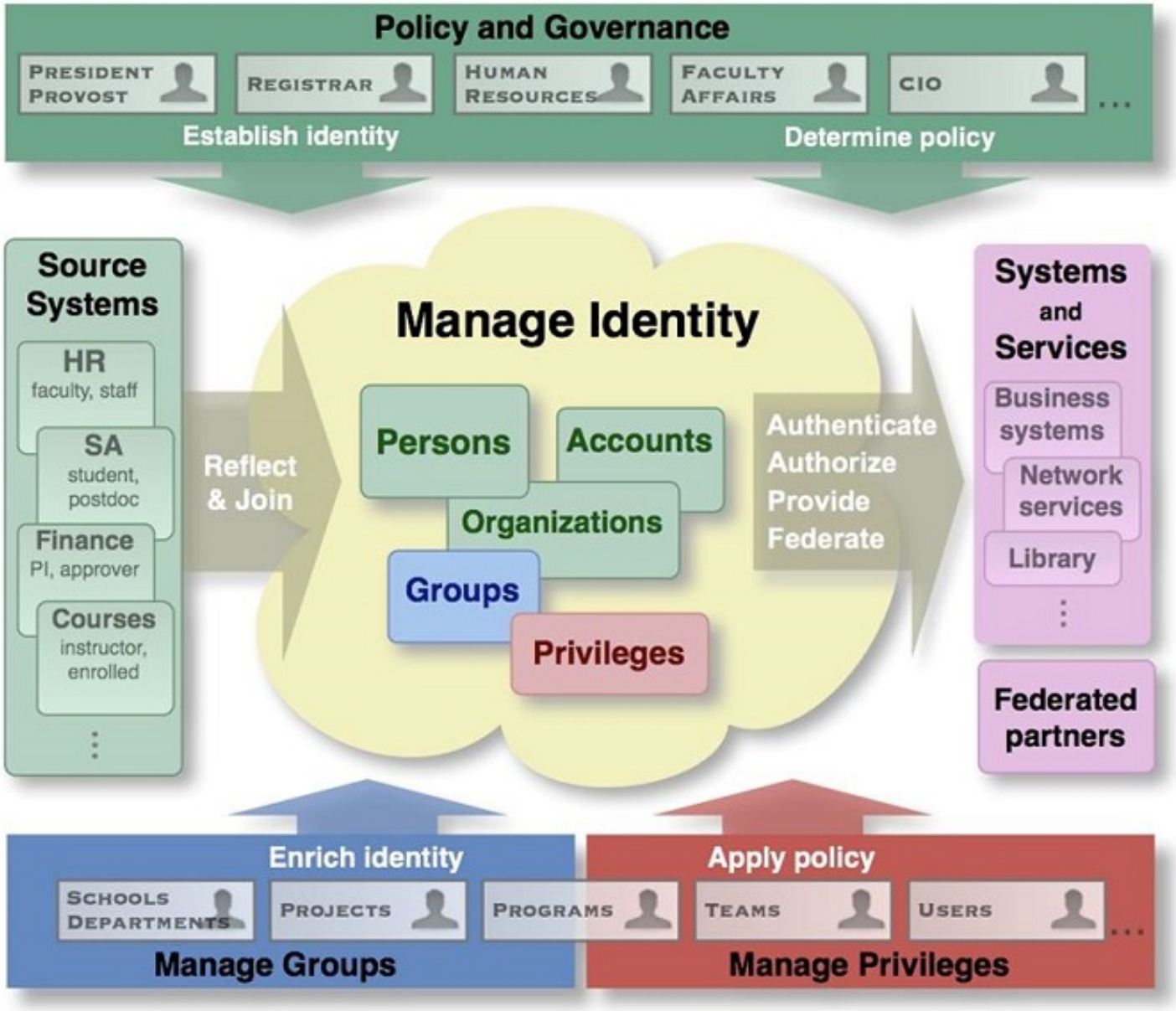
- Many universities still do…

No universal incumbent

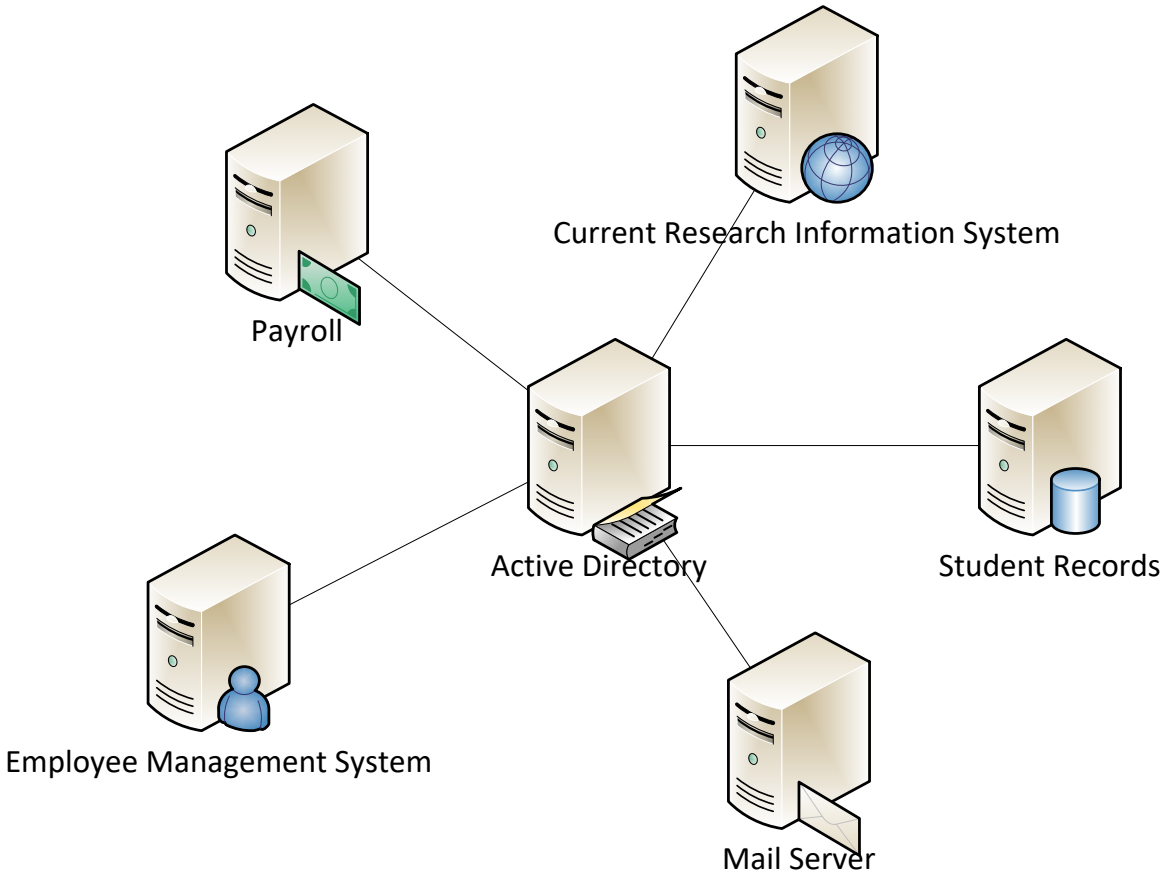
- Newer enterprise and open source efforts aimed at different scales of organisations

- In Europe and North America, some universities working together to create a “Registry for Higher Education and Research”… with mixed success.

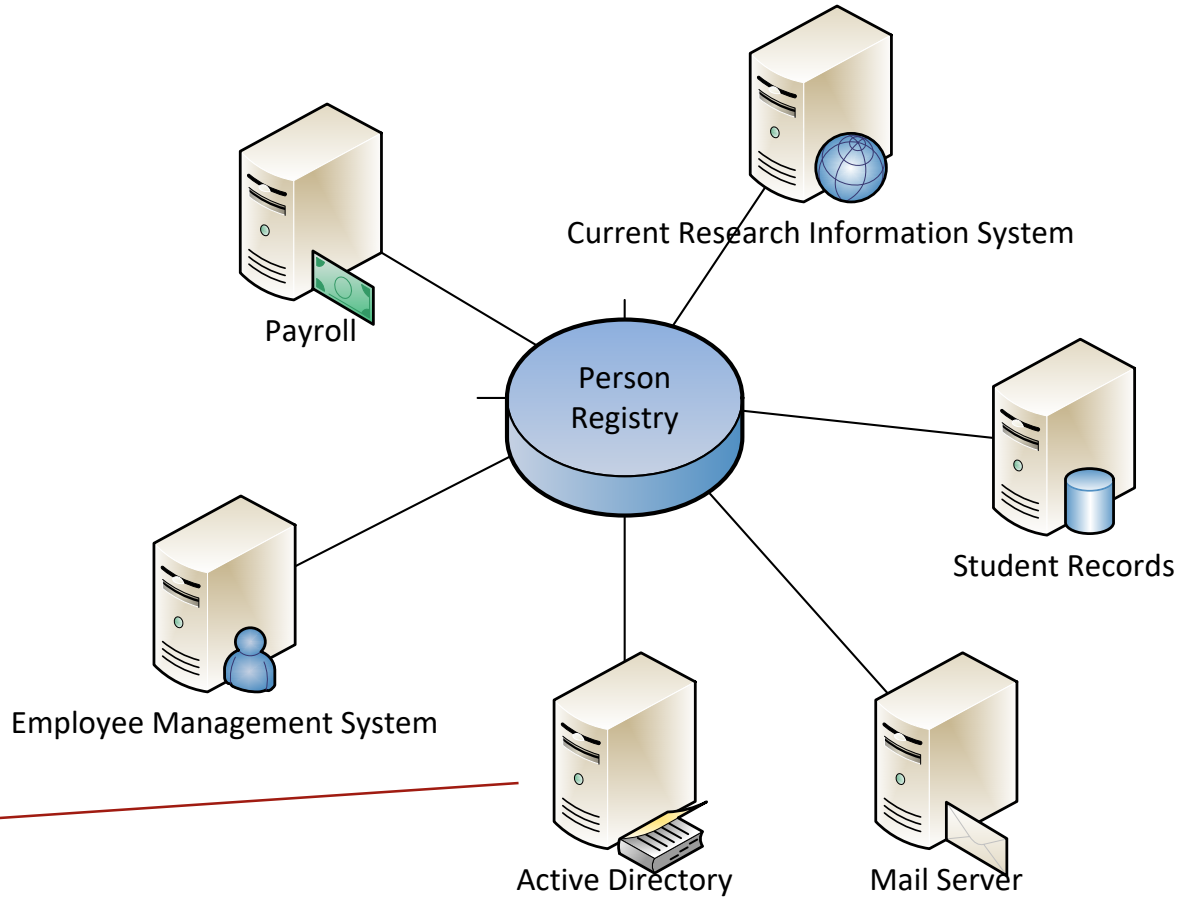
Where does the Registry sit in an Identity and Access Management Architecture?


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
Manage Groups
Apply policy
Teams
Users
Manage Privileges

What people imagine this means…

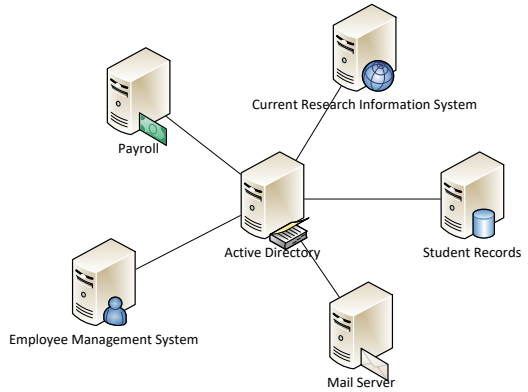


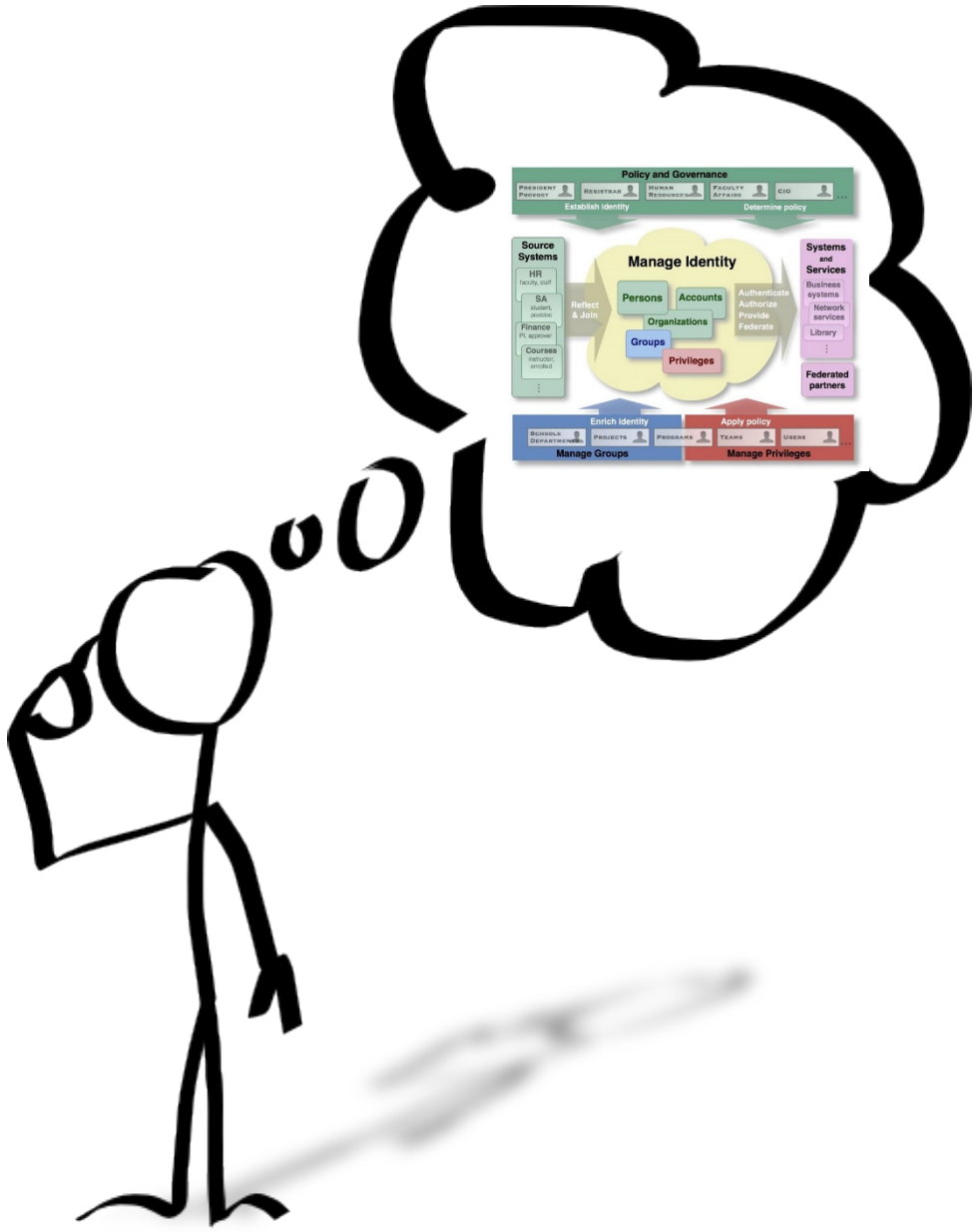
What we actually mean…



Just another consumer of identity

But how?


Payroll
Current Research Information System
Active Directory
Student Records
Employee Management System
Mail Server


Policy and Governance
Establish identity
Determine policy
Source Systems
HR
SA
Finance
Courses
Manage Identity
Persons
Accounts
Organizations
Groups
Privileges
Reflect & Join
Authenticate
Authorize
Provide
Federate
Systems and Services
Business systems
Network services
Library
Federated partners
Enrich identity
Apply policy
Manage Groups
Manage Privileges

Focus on capabilities

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

Onboarding

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

Onboarding: Enrolment

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

- Call this “administrator initiated” enrolment

Onboarding: Enrolment

- “self-signup” enrolment
  - User initiates process to create a petition
  - Usually involves filling out form(s)
  - Later the petition is (usually) reviewed and winds through an approval process

- This type of enrolment is more common in research organisations and collaborations than universities

Enrolment Capabilities

- Flexible enrolment flows
  - Administrator, self-signup, conscription
  - Simple to complex petition approval process
- Extensible collection of identifiers and attributes
- Rich and extensible set of petition states

Onboarding: consume from SOR

- Most often registry consumes electronic identity(ies) from an external System of Record
  - Employee management system
  - Student records system
  - Email management
  - National registry systems

- Quite often the single person record (entity) is constructed from multiple SOR records

Consume from SOR Capabilities

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

Matching & Linking Capabilities

- Indicate level of confidence for matches
  - No standard
  - Strive for consistency and predictability
- Provide mechanisms for handling matches
  - Automate as much as possible
  - Not every situation can be automated!

Matching & Linking Capabilities

- Flexible, rule based processing for matching and linking across multiple SOR

For students the name provided by the Registrar overrides all other name inputs.

For staff the name provided by the Human Resources overrides all other name inputs.

Identifier Capabilities

- Support a suite of common identifiers used in higher education and research
  - employee/student number
  - uid
  - email address
  - national ID
  - ORCID iD
  - eduPersonPrincipalName
  - eduPersonTargetedId
  - eduPersonUniqueId

Identifier Capabilities

- Create or “mint” new identifiers (attributes)
  - e.g. new testing service favoured by Engineering faculty requires a random 32 character [a-zA-Z0-9] identifier for each student
- Different and extensible formats
  - Random, sequential, unique, shared
- Allow self-select, but respect constraints
- Validate identifier against SOR

Lifecycle Capabilities

- Support for validity dates on persons, groups, roles
  - student role expires on 6 January 2020, but employee role has no expiration date

- Support for expiration policies including grace periods
  - on 7 January 2020, the user has at least one active role so remains active
  - grace period for student role extends until 1 March 2020 to facilitate access to final marks and transcripts

Lifecycle Capabilities

- Flexible and extensible status states
  - Active, Pending, Expired, Grace period, Suspended, Approved, Pending approval, Confirmed, Invited, Denied, Declined, Deleted, Duplicate

Provisioning

- Provisioning refers to the action of using Registry data to create or remove access to applications and services
- Three usual provisioning mechanisms:
  1. Push Provisioning
  2. Pull Provisioning
  3. Messaging

Provisioning Capabilities

- Automated provisioning
- Manual (re-)provisioning
- Support for multiple and varied provisioning targets
- Plugin or other mechanisms to add custom provisioners

Group Registries

Group Registry manages groups of entities/people

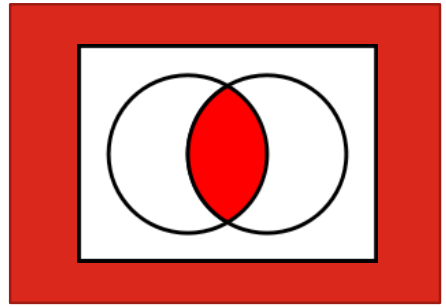
Group Registry Capabilities

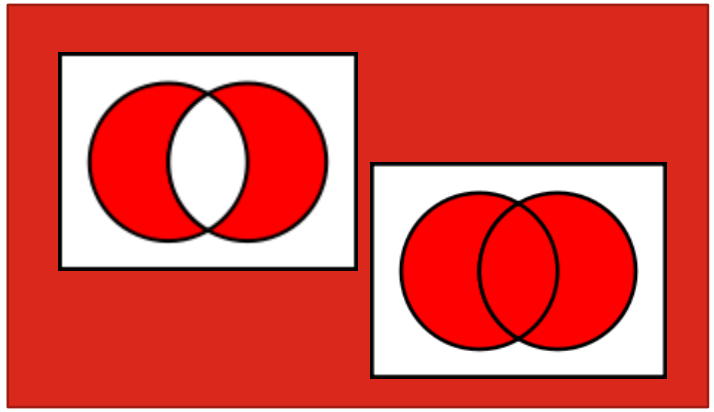
- Basic group capabilities
  - Name, description, members, owners
  - Validity dates on membership
  - Open (self-service) vs closed (managed)
  - Delegated administration

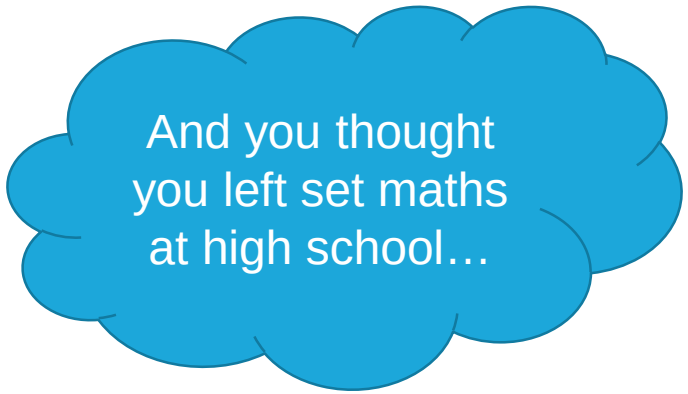
- Groups, Roles, Permissions

Group Registry Capabilities

- Advanced capabilities:
  - Groups of groups (union)
  - Intersection
  - Composition
  - Provisioning







Successful Registries

Strategies to help make your registry a success

Strategies for success

- Respect the SOR data (and its owner)
  - SOR data can be messy
  - Take it as it comes and follow the robustness principle

> “Be conservative in what you send,
> be liberal in what you accept”
>
> *– Postel’s law*

Strategies for success

- Add value where possible to the other SOR
  - Often the data in the Identity Registry can be more refined and ultimately more useful
  - Work with SOR owners to see if they can benefit from receiving data back from the registry

Some tools to consider…

(a non-exhaustive list)

COmanage

- Open Source from Internet2/InCommon in USA
- Adopted by Internet2 TIER programme

- “… a tool for identity enrolment and lifecycle management of people associated with your organisation. Suitable for small collaborations with tens of people or large universities with hundreds of thousands… allows you to organise complex identity data from multiple sources to create a single view of a person.”

https://www.internet2.edu/products-services/trust-identity/comanage/

midPoint

- Open Source from Evolveum
- Adopted by Internet2 TIER programme

- “Features of midpoint include identity governance, provisioning and audits, organisation structure, entitlement management, credential management, and workflow.”

https://evolveum.com/midpoint/

WSO2 Identity Server

- Open Source from WSO2

- “WSO2 Identity Server…is a uniquely flexible, open source IAM product optimised for identity federation and SSO with comprehensive support for adaptive and strong authentication.”

https://wso2.com/identity-and-access-management/

KeyCloak

- Open Source 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 the box. You’ll even get advanced features such as User Federation, Identity Brokering and Social Login.”

https://www.keycloak.org/

OpenIAM

- Community edition is Open Source

- “The OpenIAM Identity Manager automats 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.”

https://www.openiam.com/

Apache Syncope

- Open Source from Apache Foundation

- “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.”

https://syncope.apache.org/

OpenAM

OpenAM
COMMUNITY EDITION

- “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. OpenAM originated as OpenSSO, an access management system created by Sun Microsystems and now owned by Oracle Corporation.”

https://github.com/OpenIdentityPlatform/OpenAM/

Microsoft Identity Manager

- “On-premises identity and access management. Synchronises identities between directories, databases and apps. Administer self-service password, group and certificate management. Increase admin security with polices, privileged access and roles.”

https://www.microsoft.com/en-us/cloud-platform/microsoft-identity-manager

NetIQ Identity Manager

- “The comprehensive solution for provisioning identity and controlling access, Identity Manager delivers a complete, yet affordable solution to control who has access to what inside 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.”

- (formally Novell)

https://www.netiq.com/products/identity-manager/advanced/

IBM Tivoli Identity Manager

- “Automatically create, manage, and delete user access to various system resources such as files, servers, applications, and more based on job roles or requests.”

www-01.ibm.com/software/tivoli/products/identity-mgr-express/

Oracle Identity Manager

ORACLE®

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

https://docs.oracle.com/cd/E52734_01/oim/index.html

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.”

https://www.forgerock.com/platform