

OpenSource Identity Registries And the IdMS Ecosystem: *I.D. Happened One Night*

Benjamin Oshrin
The Oshrinium LLC

Jeremy Rosenberg
Simon Fraser University

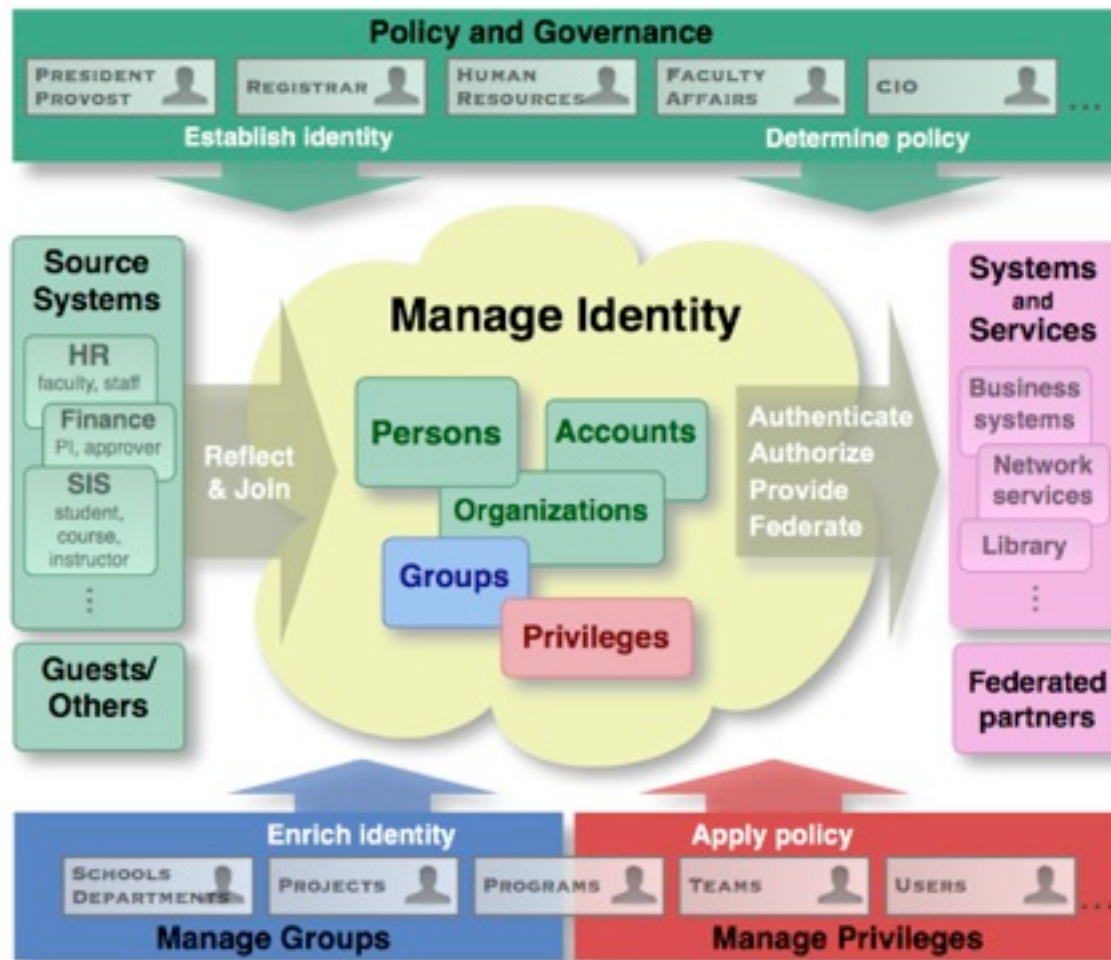
Table of Contents

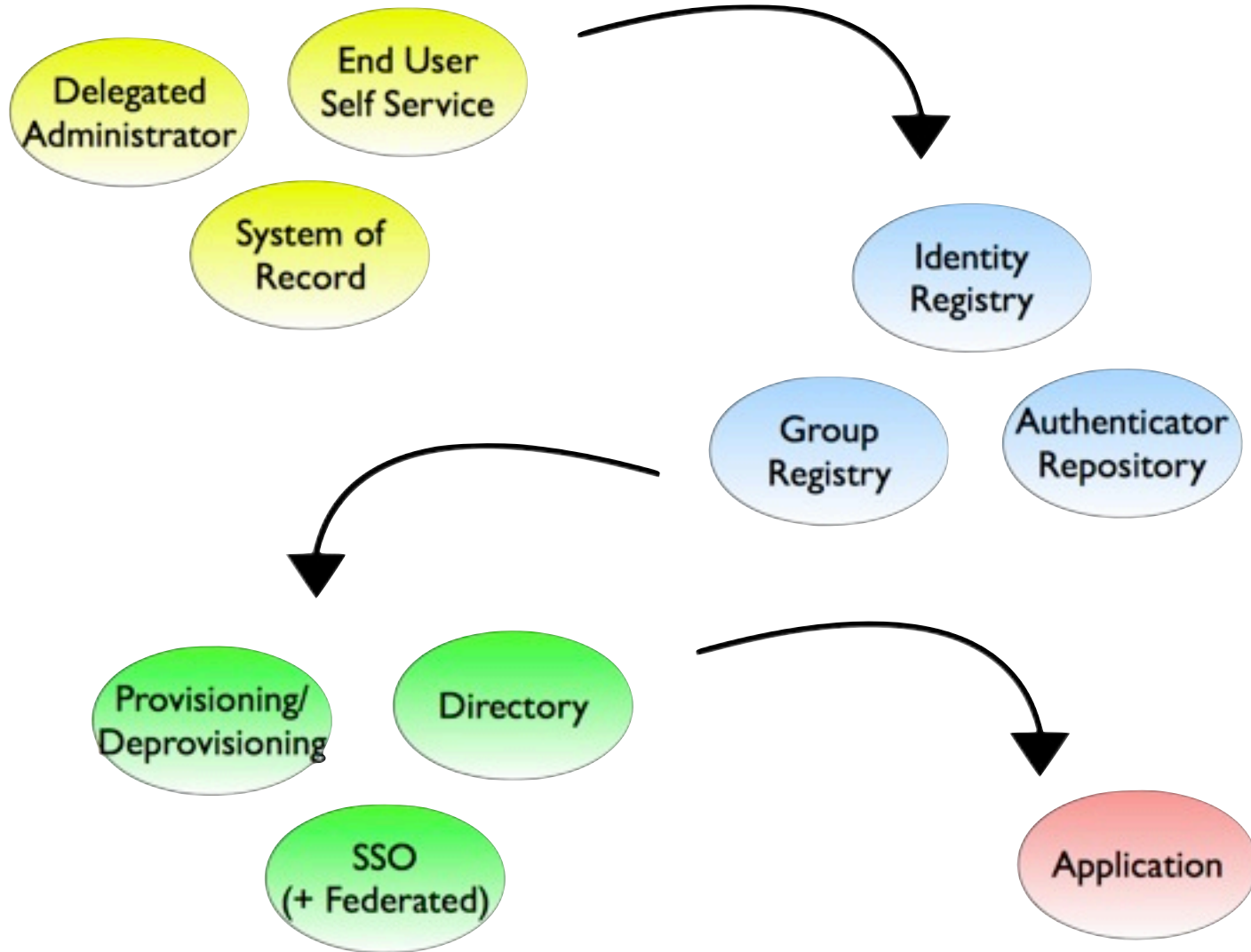
- Identity Registries & The IdMS Ecosystem
- For the Enterprise: OpenRegistry
- For Virtual Organizations: COmanage

Why OpenSource?

- In the end, we own the product and have a vested interest in it
 - Higher ed institutions have been around a lot longer than our vendors
- Good luck getting a bug fix from a vendor
- Better products evolve from broader participation

I2 Identity & Access Management Model



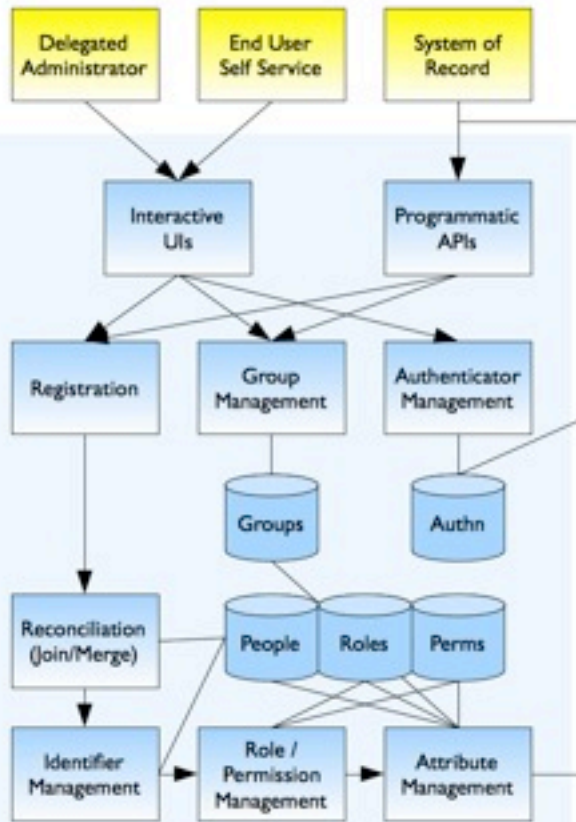


What's an Identity Registry?

- A single repository of identity data about all individuals associated with an institution
- May be sourced from multiple authoritative systems of records
- Adds value by collating data and executing business rule-based data transformations
- Publishes data to downstream systems and applications
- A black box
- Plumbing (er, infrastructure)

OpenSource Identity Registries

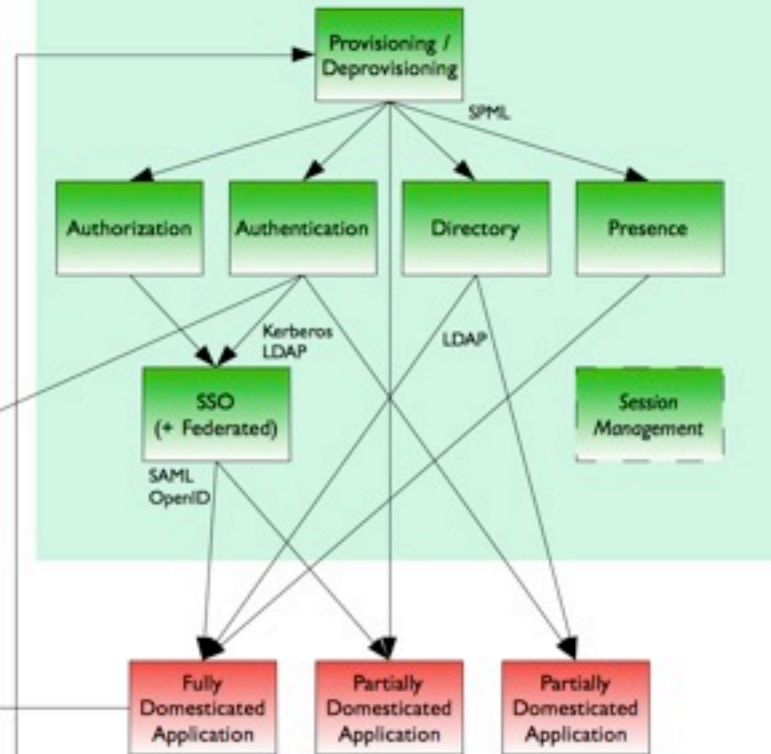
Enterprise Identity Management
Reference Architecture, July 2010



Identity Data Management System
•Collate and add value to authoritative data

Identity Services

•Read-mostly identity data for application use



Registries, LOA, and Social Identity

- Certain LOA factors can be stored in a Registry (eg: identity proofing)
- Social Identities often have low(er) LOA
- Can still link Social Identity to Institutional Identity via Registry
- Run-time LOA may be affected

About OpenRegistry

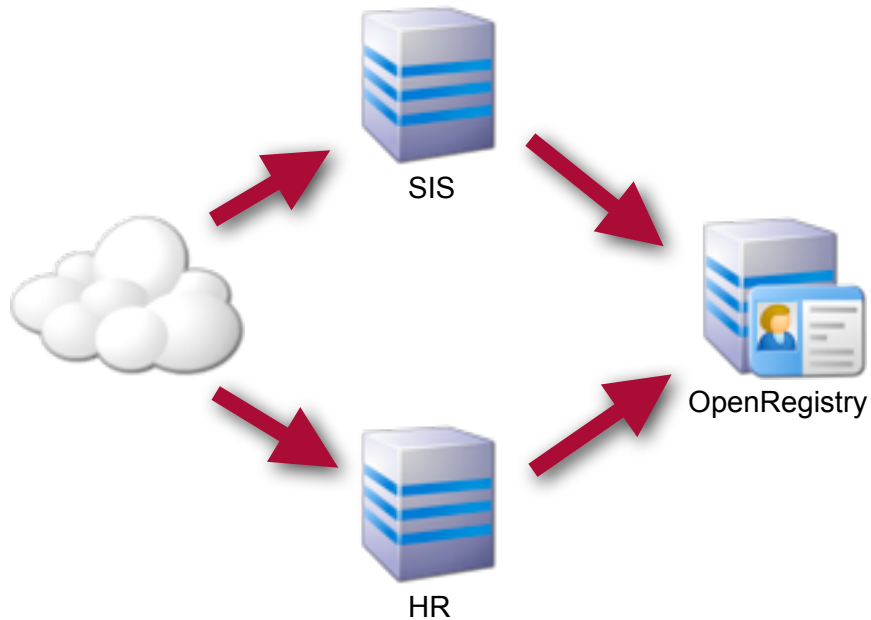
- An open source Identity Management system
- A place for data about people affiliated with your institution
- Combines distributed information into single identity records
- Identity store, but generally NOT authoritative
- Identity reconciliation for multiple SoRs
- Identifier assignment
- Input
 - web, batch and REST interfaces from SoRs
- Output
 - queues, REST, batch, report server, Directory Builder
- *OpenRegistry Session Tuesday at 2pm

OpenRegistry Overview

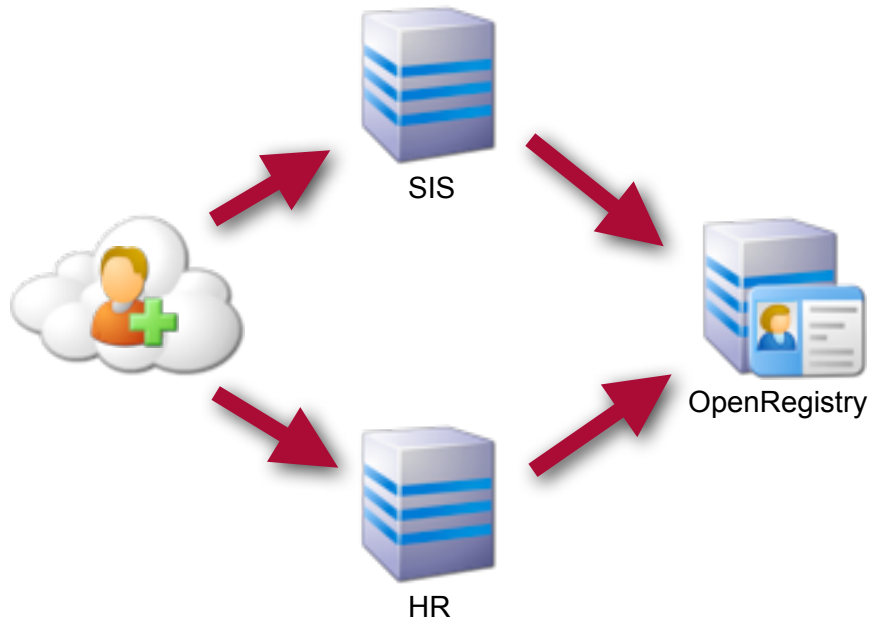
OpenRegistry Overview



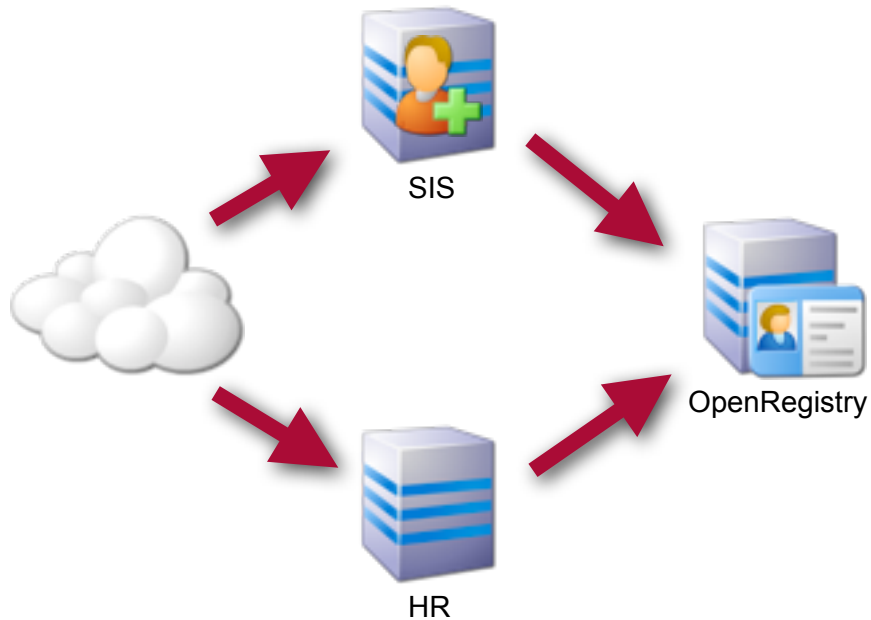
OpenRegistry Overview



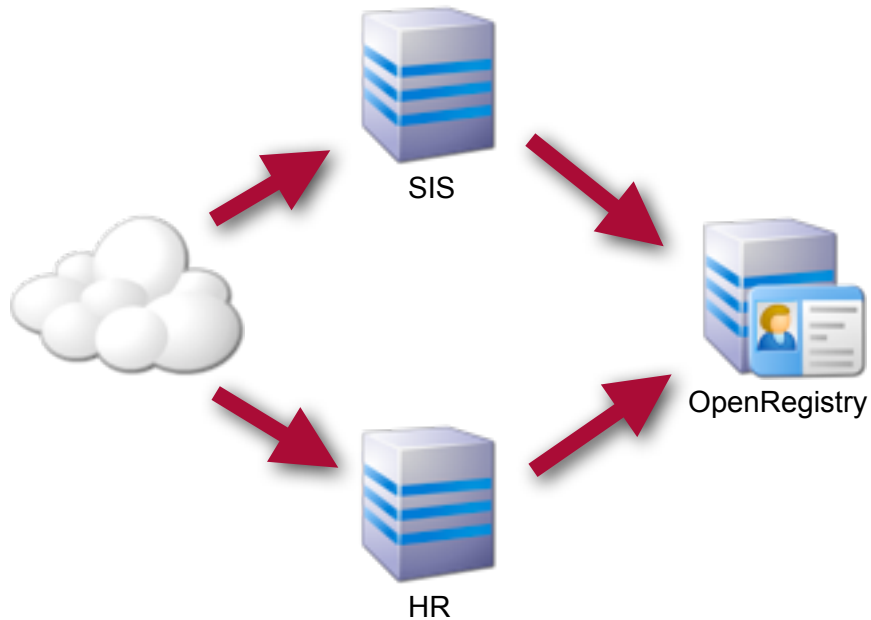
OpenRegistry Overview



OpenRegistry Overview




OpenRegistry Overview

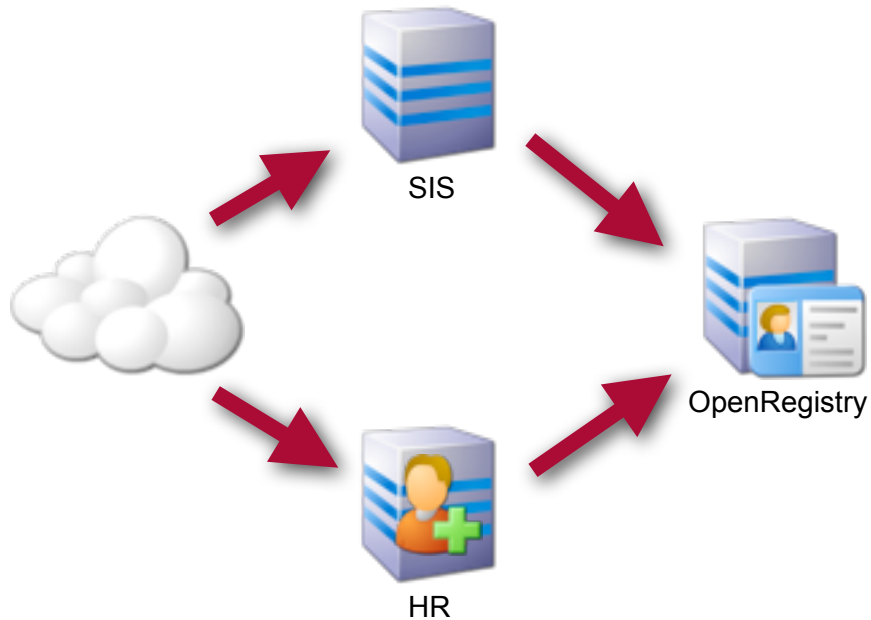


Kipling, Rudyard

Undergrad




OpenRegistry Overview

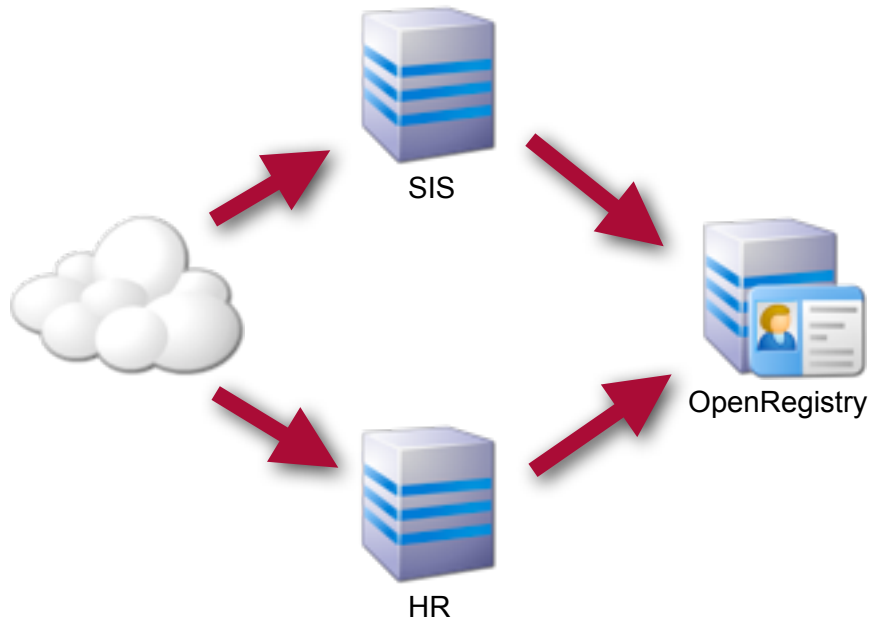


Kipling, Rudyard

Undergrad



OpenRegistry Overview

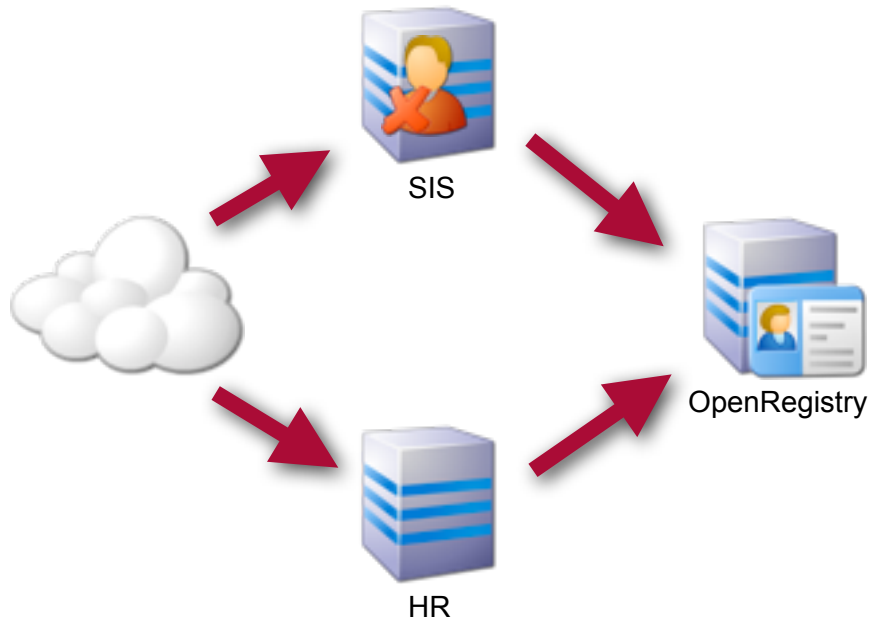


Kipling, Rudyard

Undergrad
Staff




OpenRegistry Overview

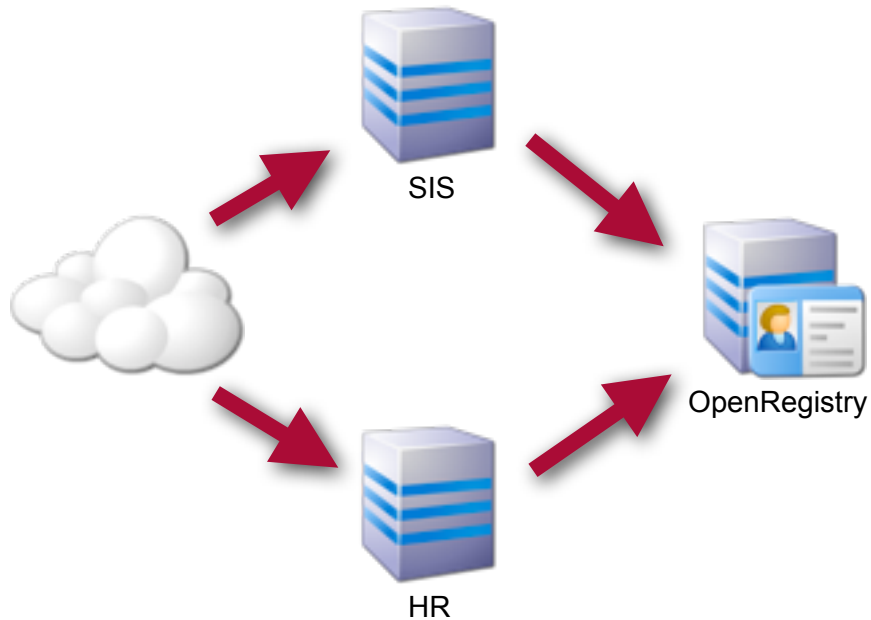


Kipling, Rudyard

Undergrad
Staff



OpenRegistry Overview

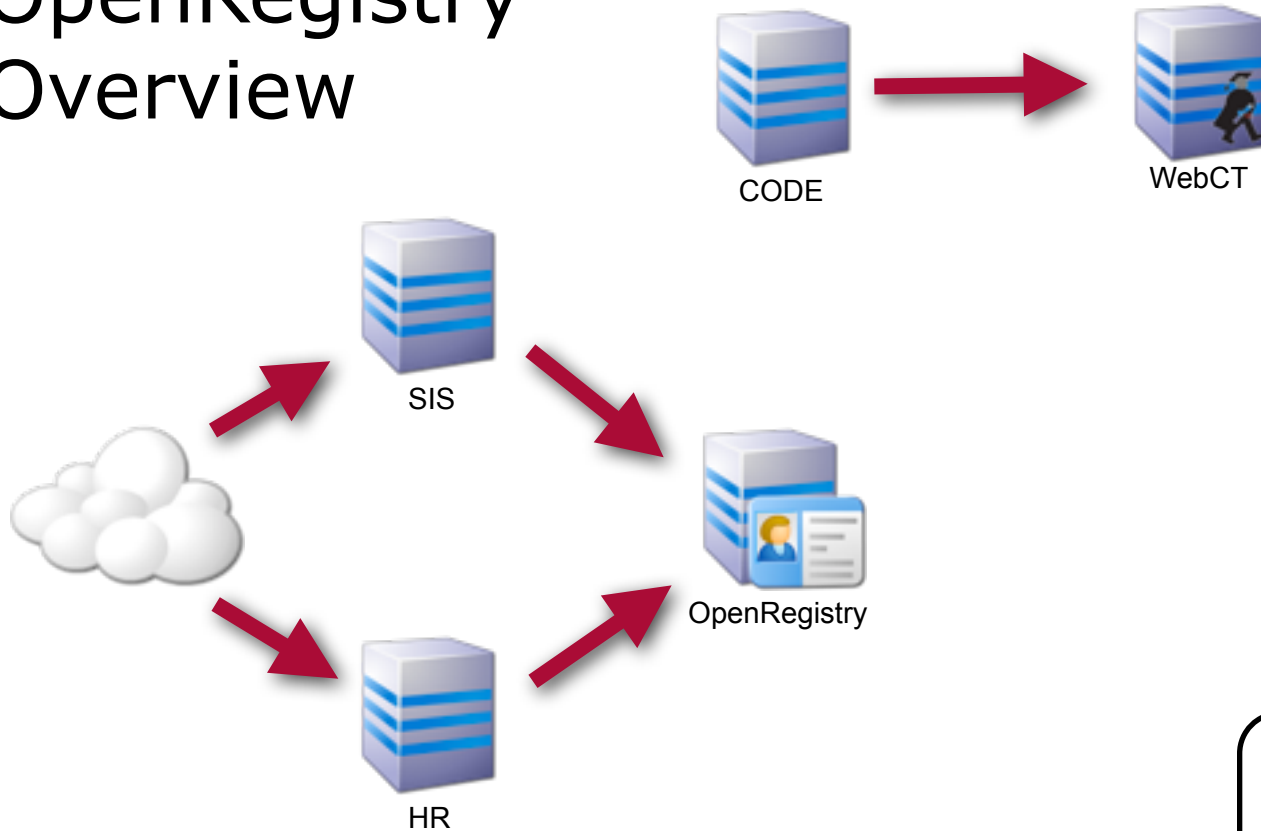


Kipling, Rudyard

Former Undergrad
Staff



OpenRegistry Overview

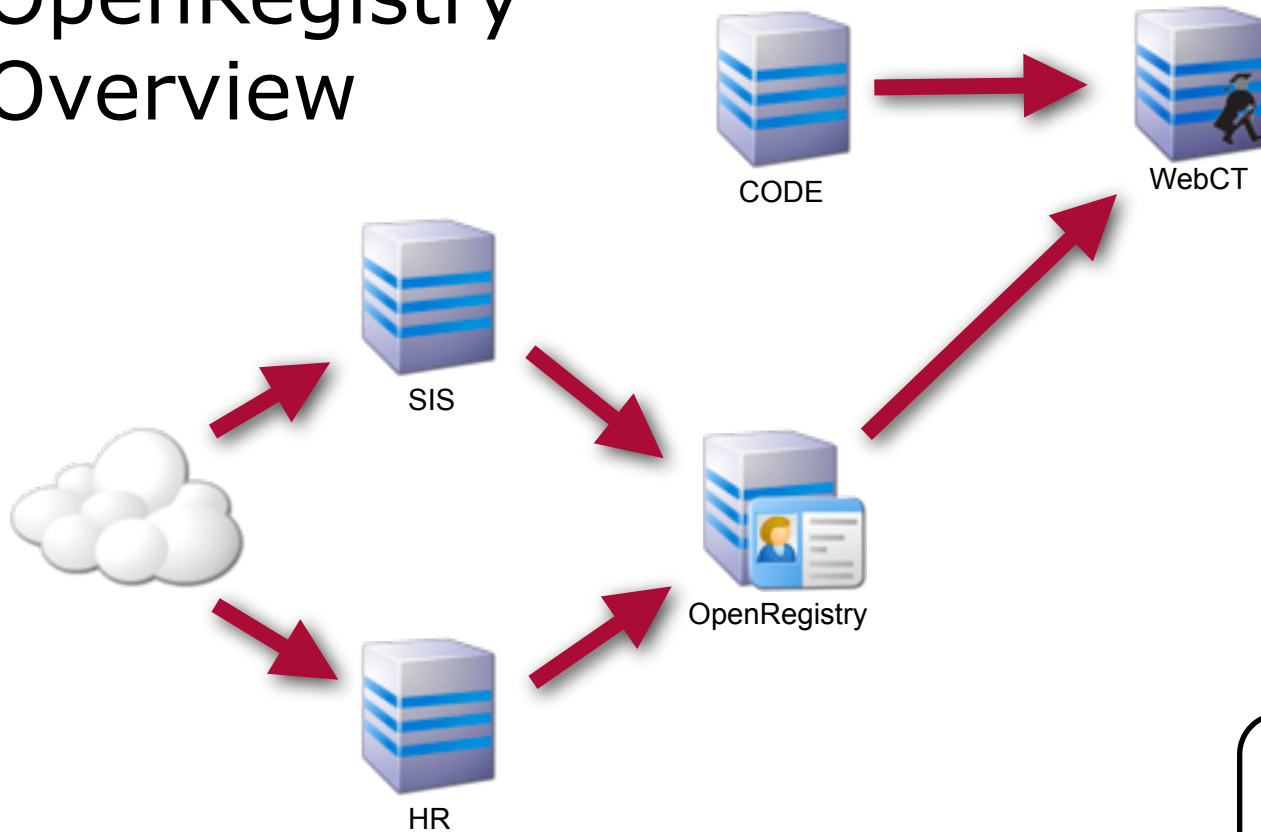


Kipling, Rudyard

Former Undergrad
Staff



OpenRegistry Overview

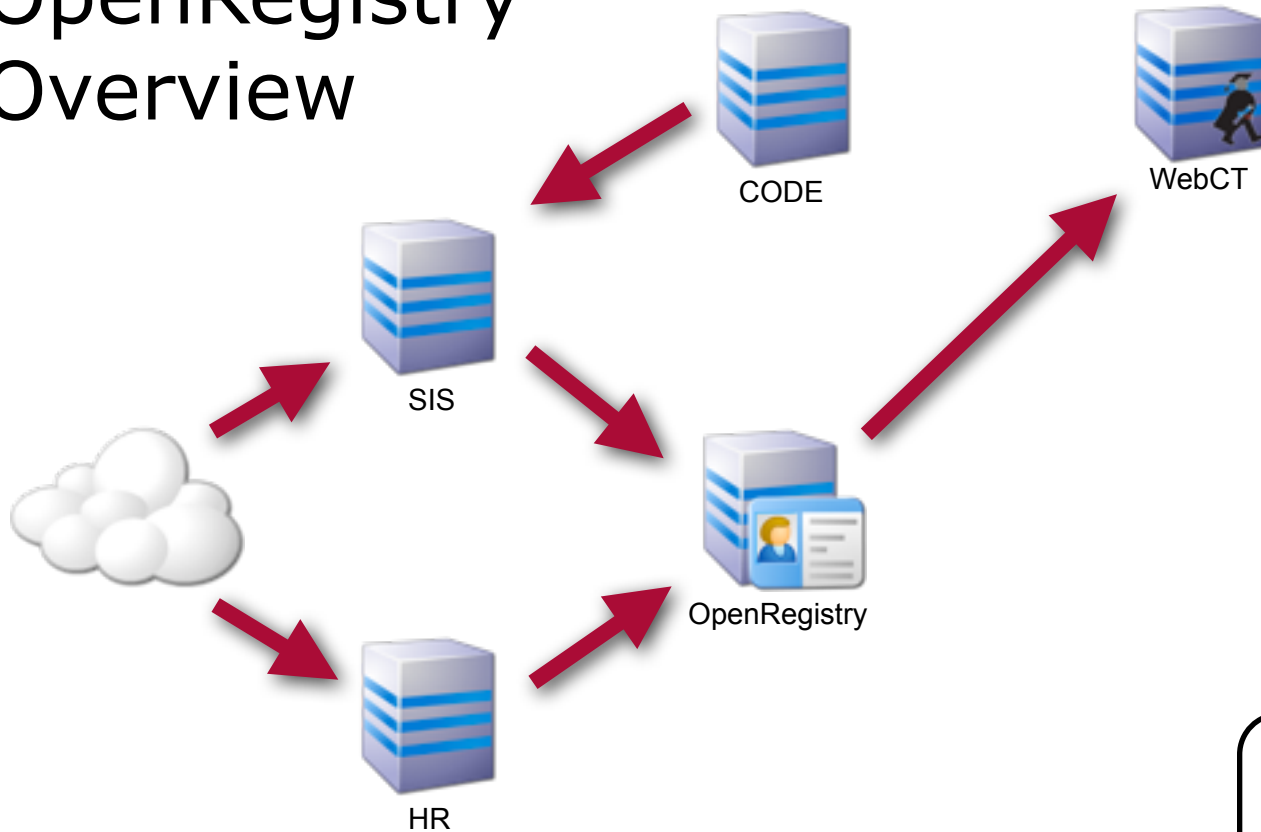


Kipling, Rudyard

Former Undergrad
Staff



OpenRegistry Overview

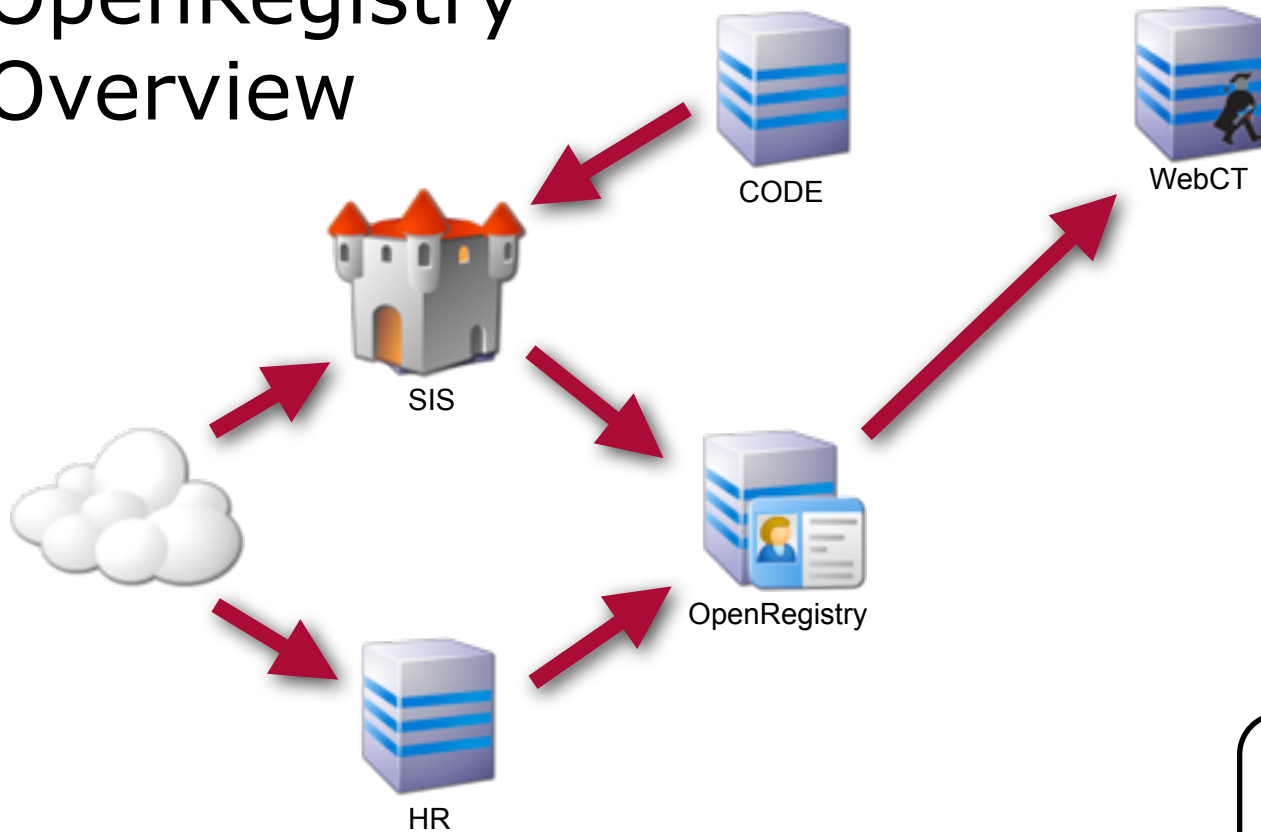


Kipling, Rudyard

Former Undergrad
Staff



OpenRegistry Overview

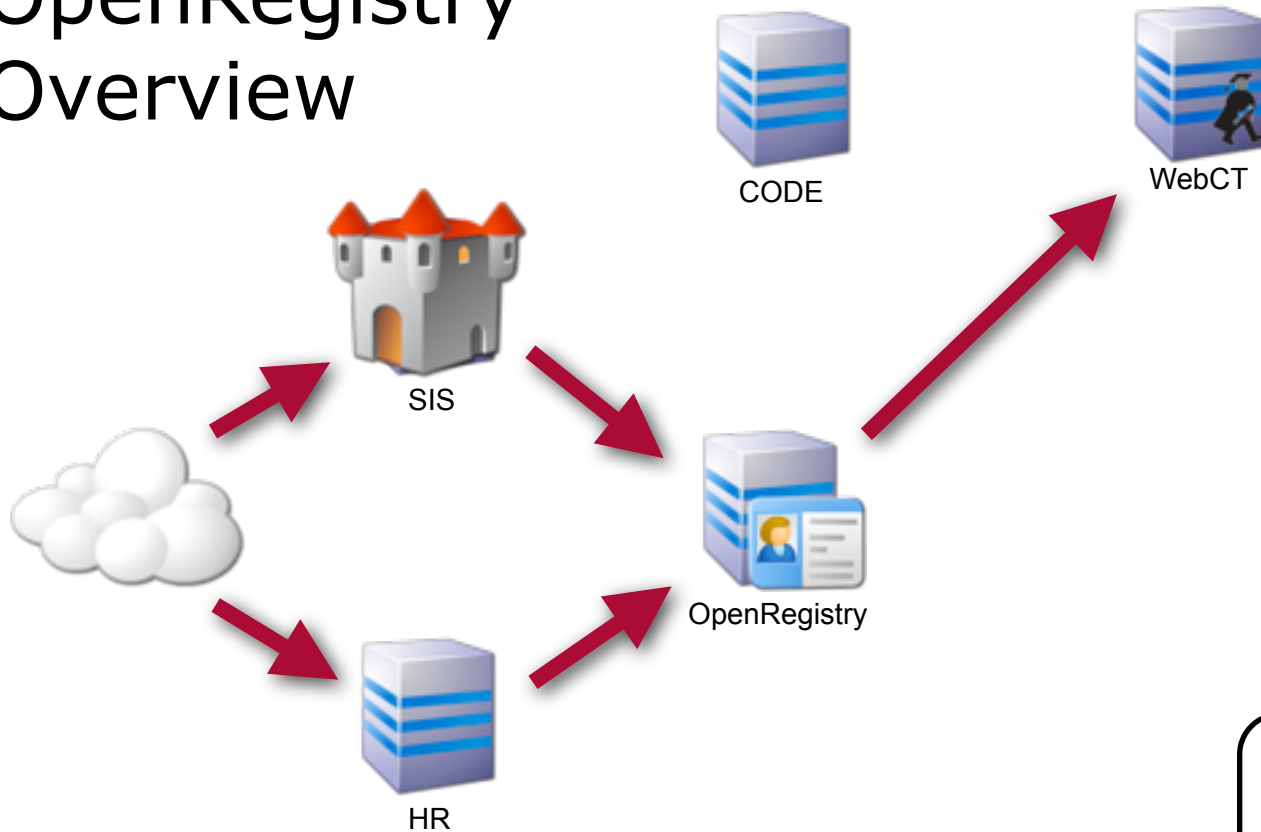


Kipling, Rudyard

Former Undergrad
Staff



OpenRegistry Overview

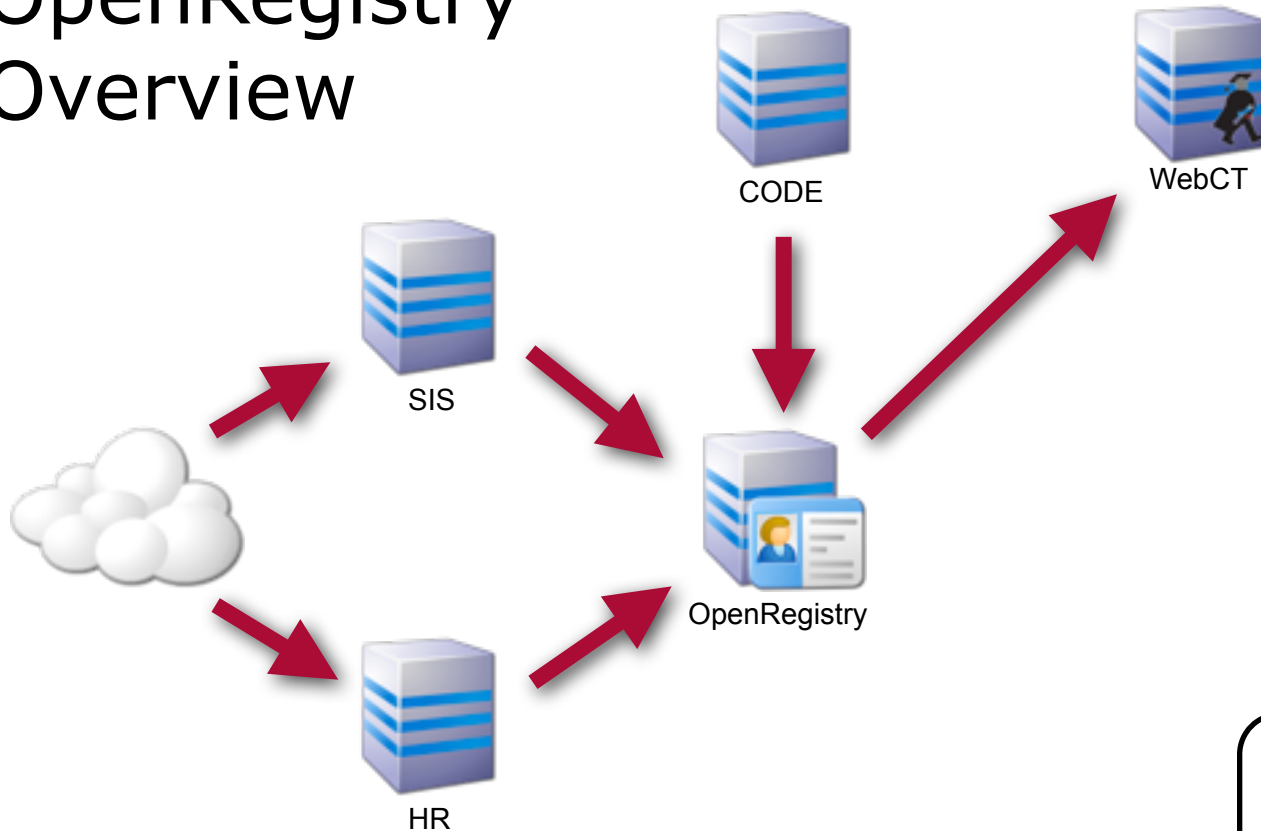


Kipling, Rudyard

Former Undergrad
Staff



OpenRegistry Overview

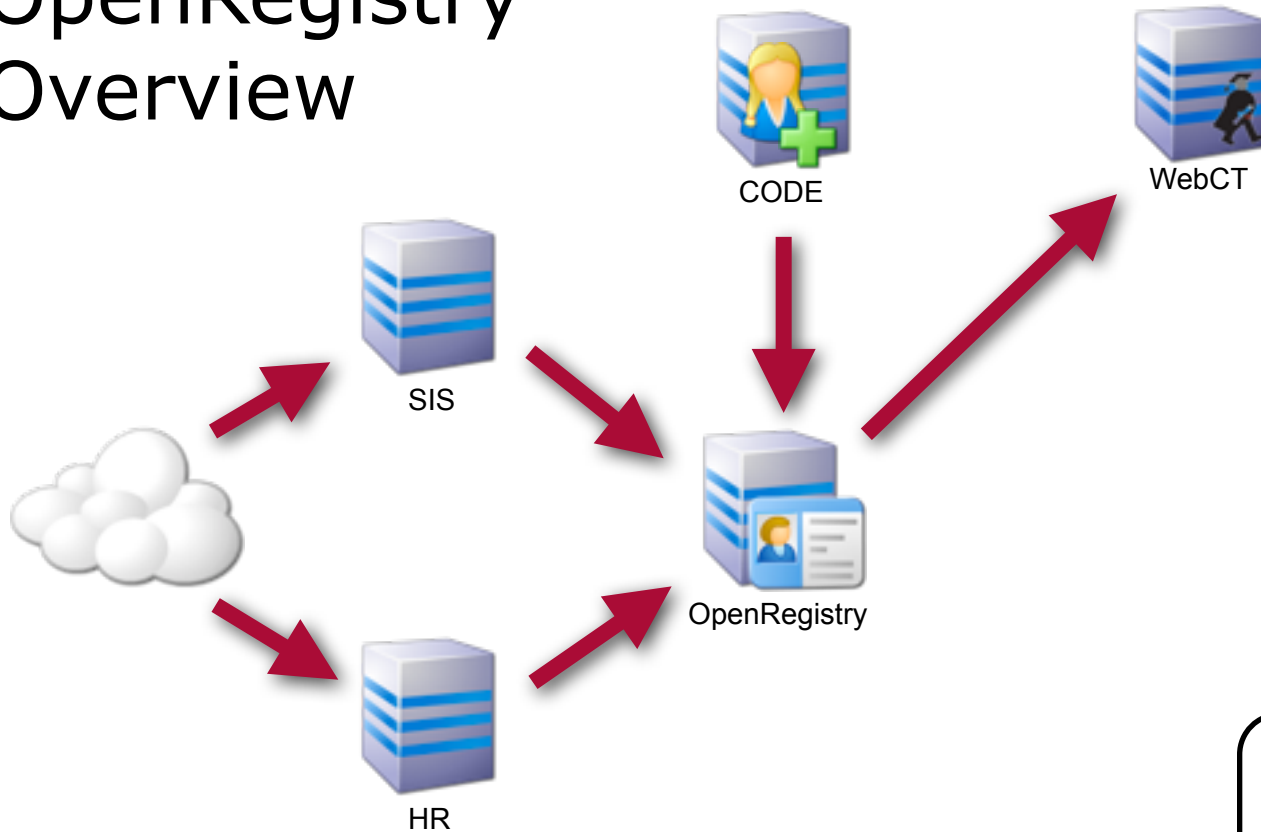


Kipling, Rudyard

Former Undergrad
Staff



OpenRegistry Overview

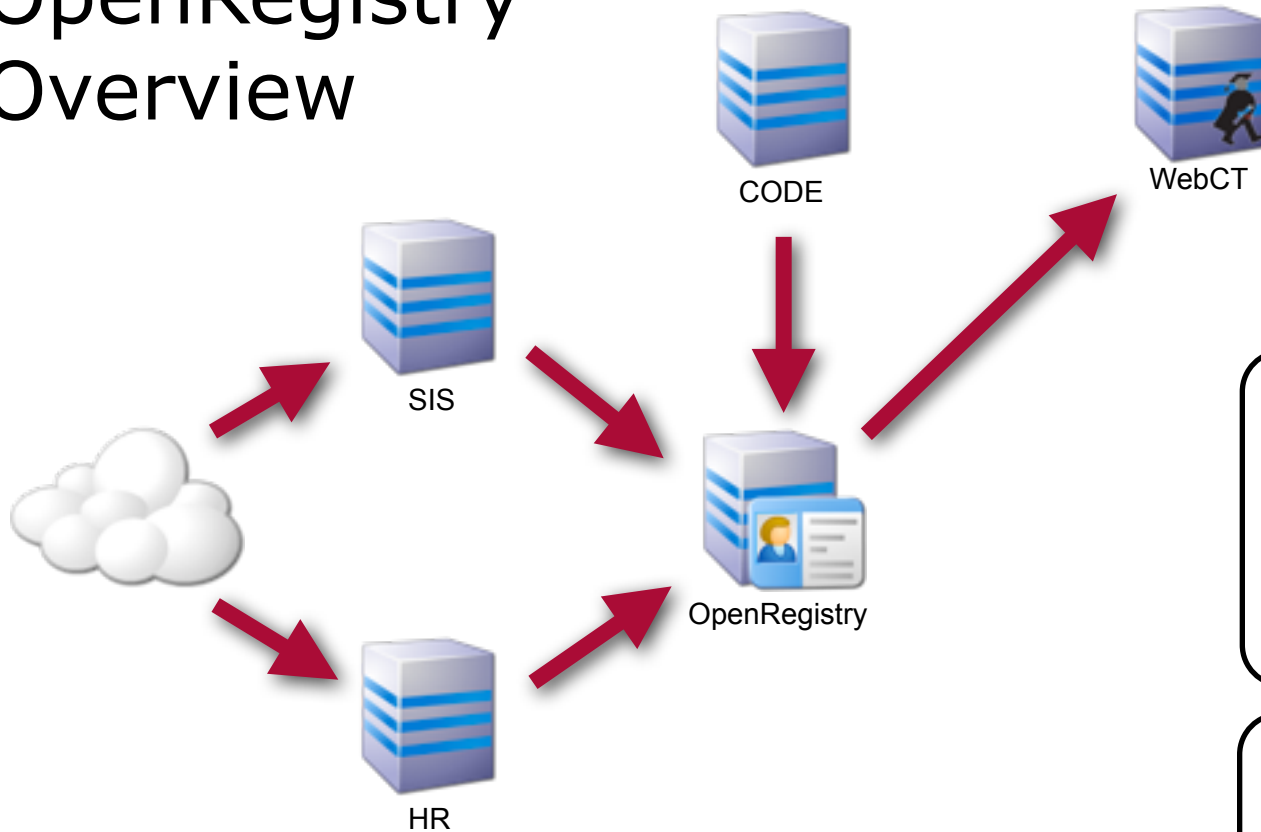


Kipling, Rudyard

Former Undergrad
Staff

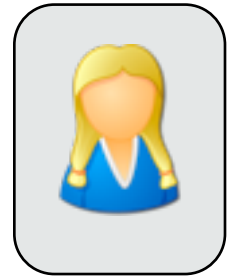


OpenRegistry Overview



Bronte, Emily

CODE

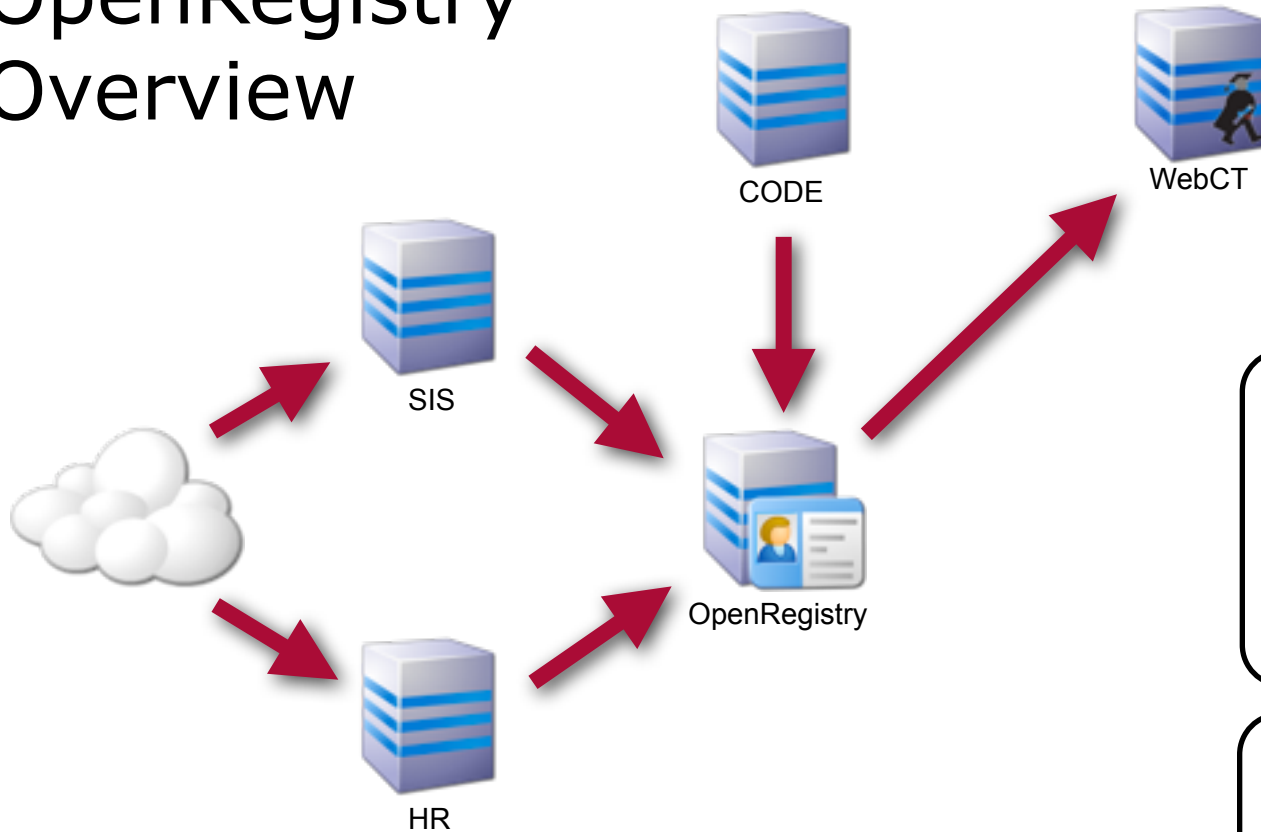


Kipling, Rudyard

Former Undergrad
Staff



OpenRegistry Overview



Bronte, Emily

CODE **Expired**

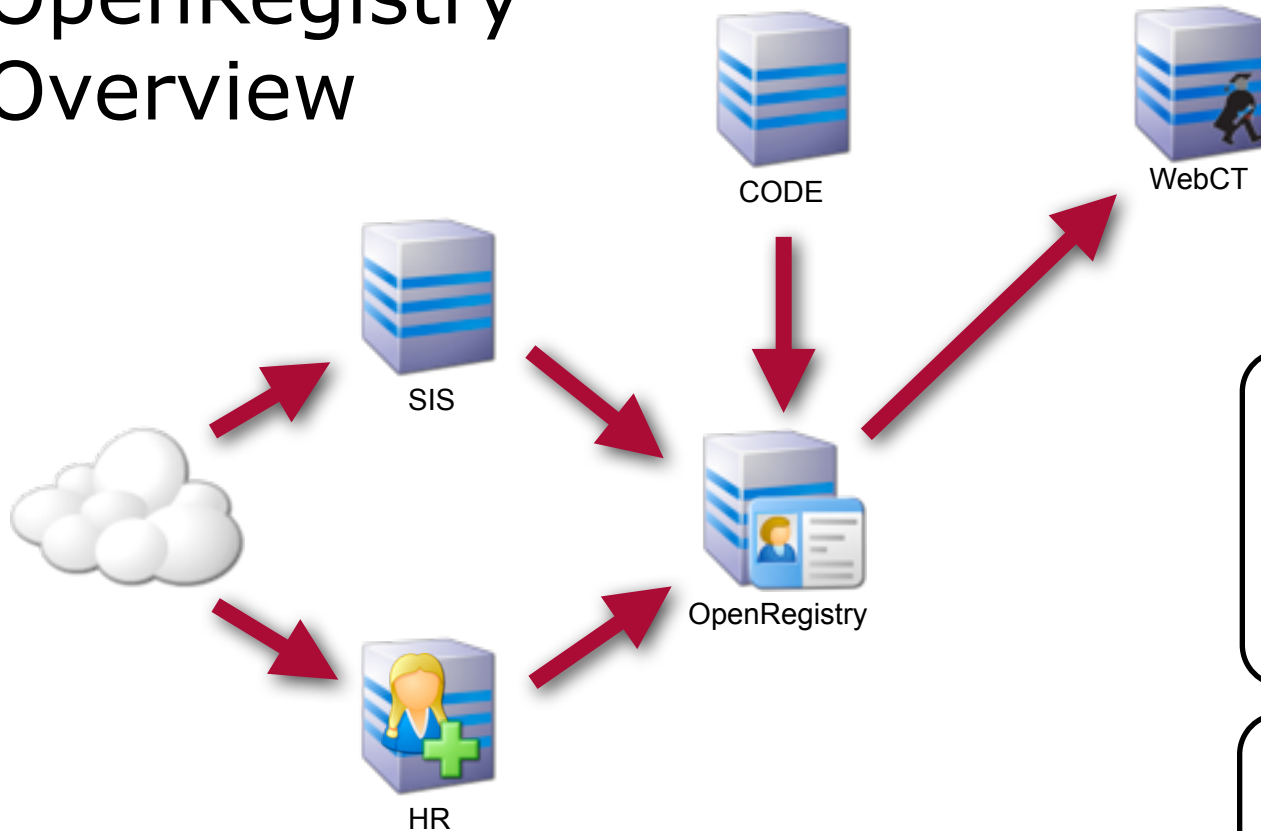


Kipling, Rudyard

Former Undergrad
Staff

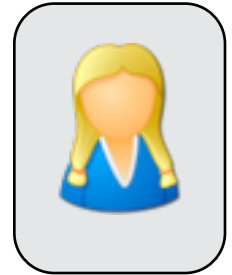


OpenRegistry Overview



Bronte, Emily

CODE **Expired**

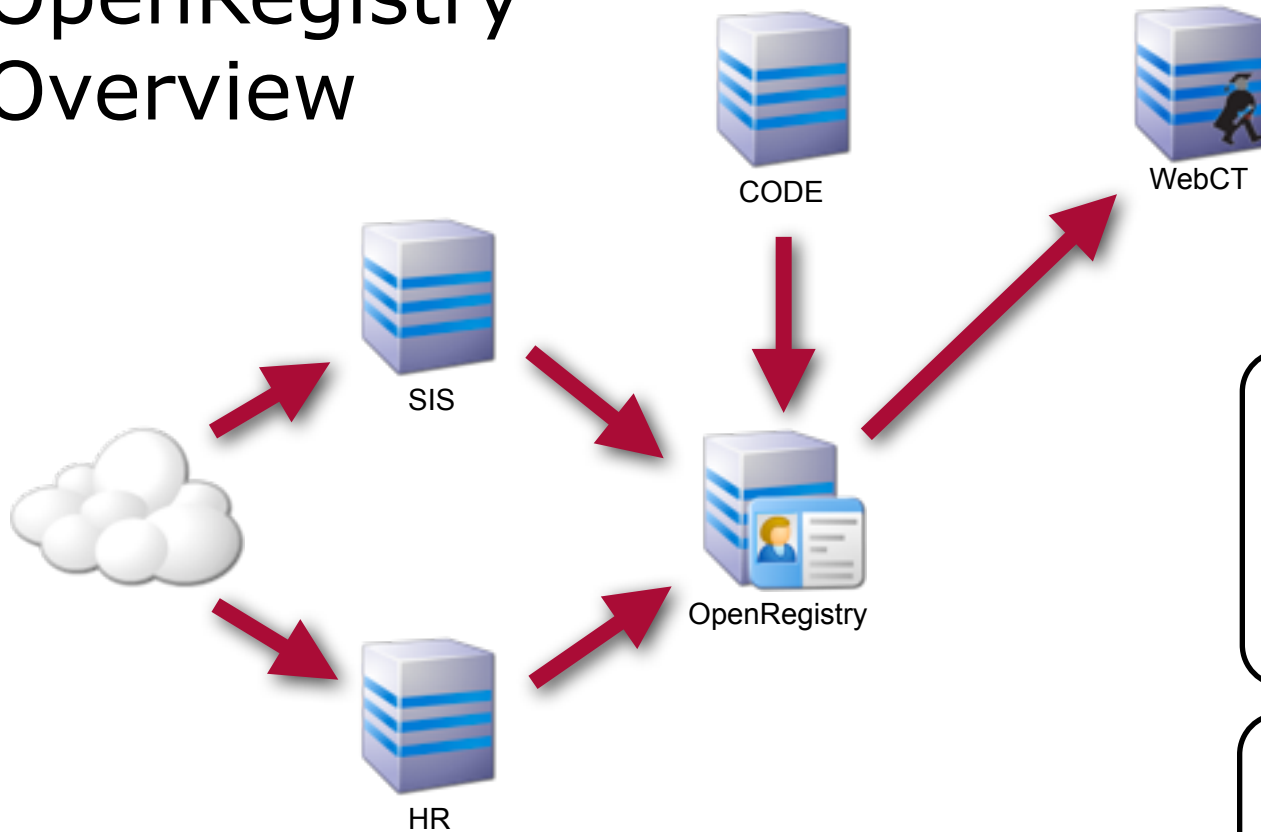


Kipling, Rudyard

Former Undergrad
Staff

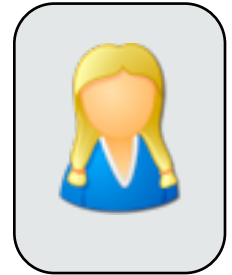


OpenRegistry Overview



Bronte, Emily

CODE **Expired**
Faculty

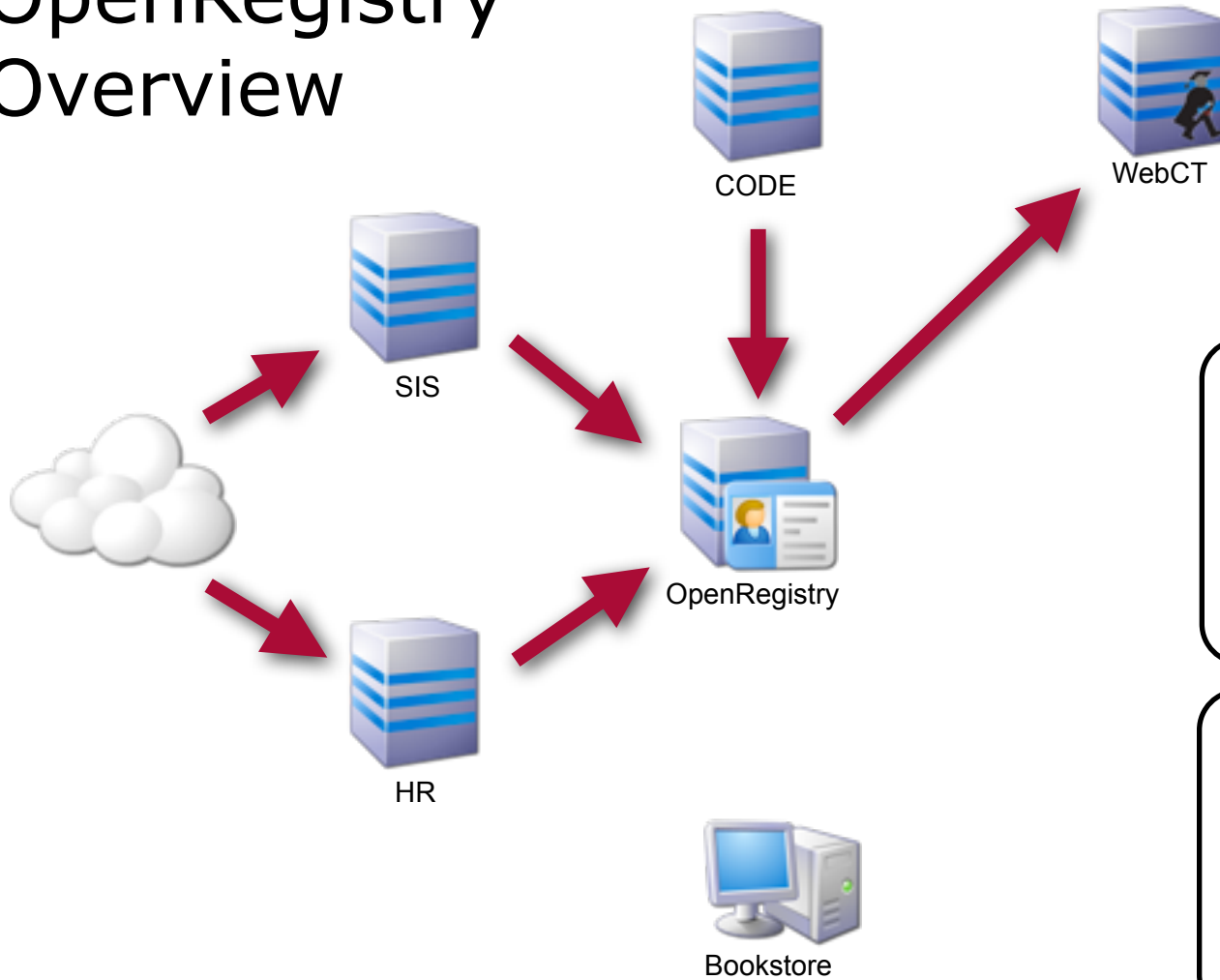


Kipling, Rudyard

Former Undergrad
Staff

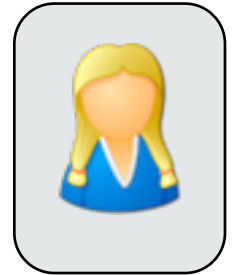


OpenRegistry Overview



Bronte, Emily

CODE **Expired**
Faculty

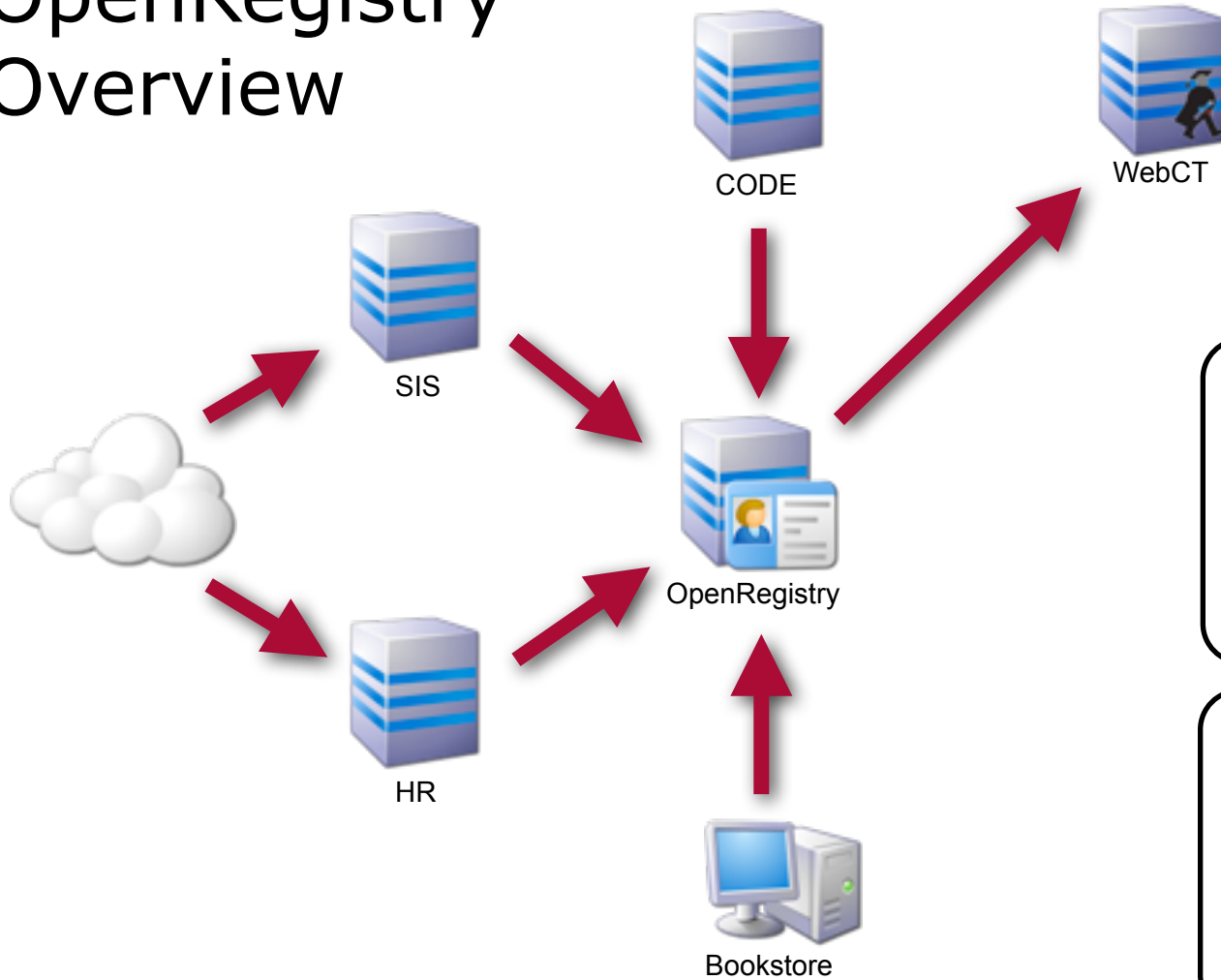


Kipling, Rudyard

Former Undergrad
Staff

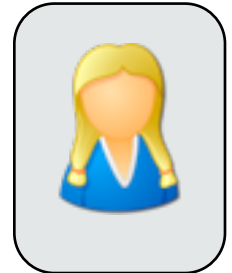


OpenRegistry Overview



Bronte, Emily

CODE **Expired**
Faculty

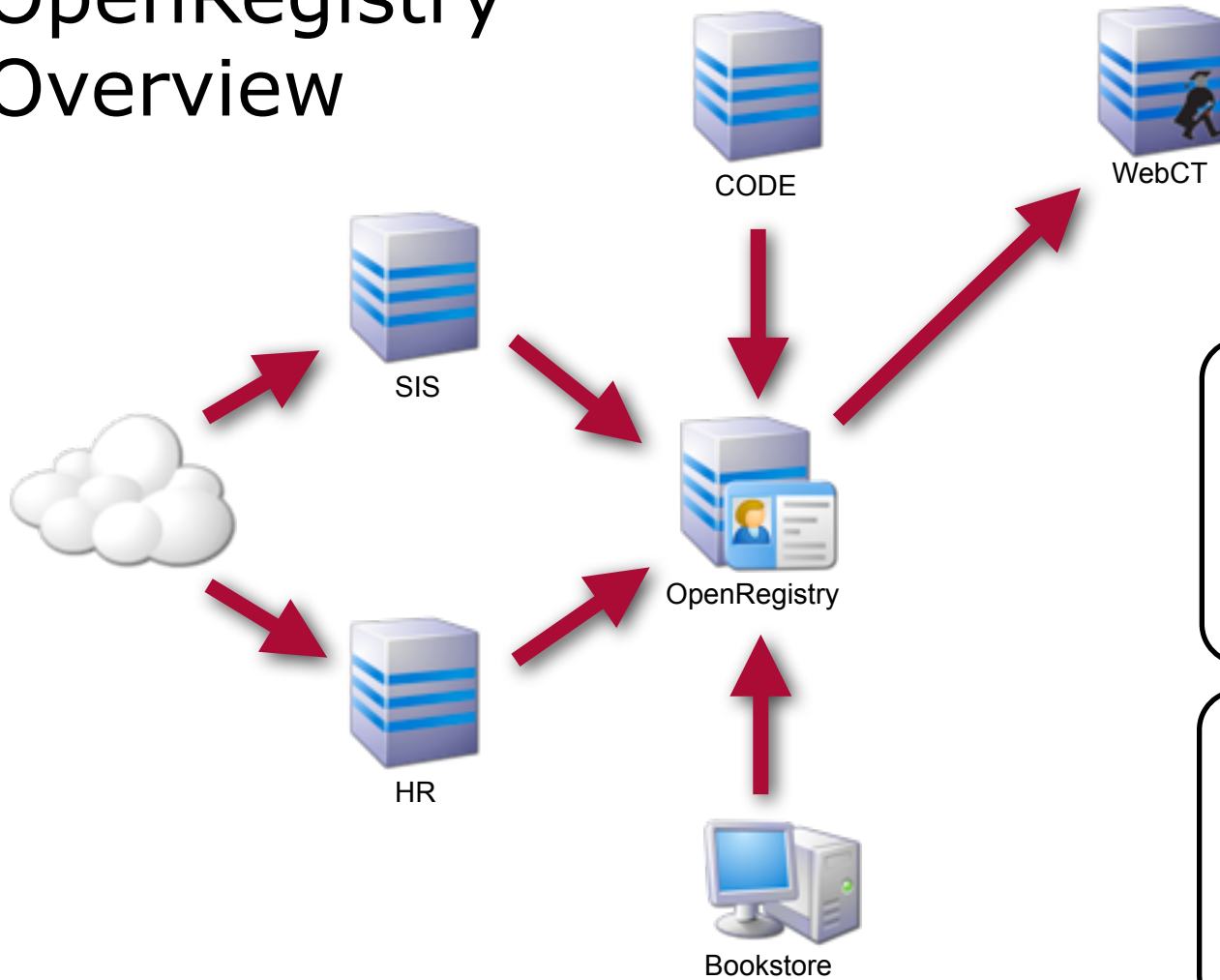


Kipling, Rudyard

Former Undergrad
Staff

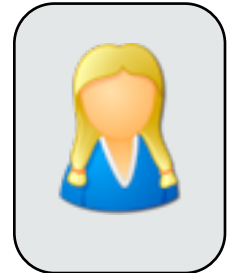


OpenRegistry Overview



Bronte, Emily

CODE **Expired**
Faculty



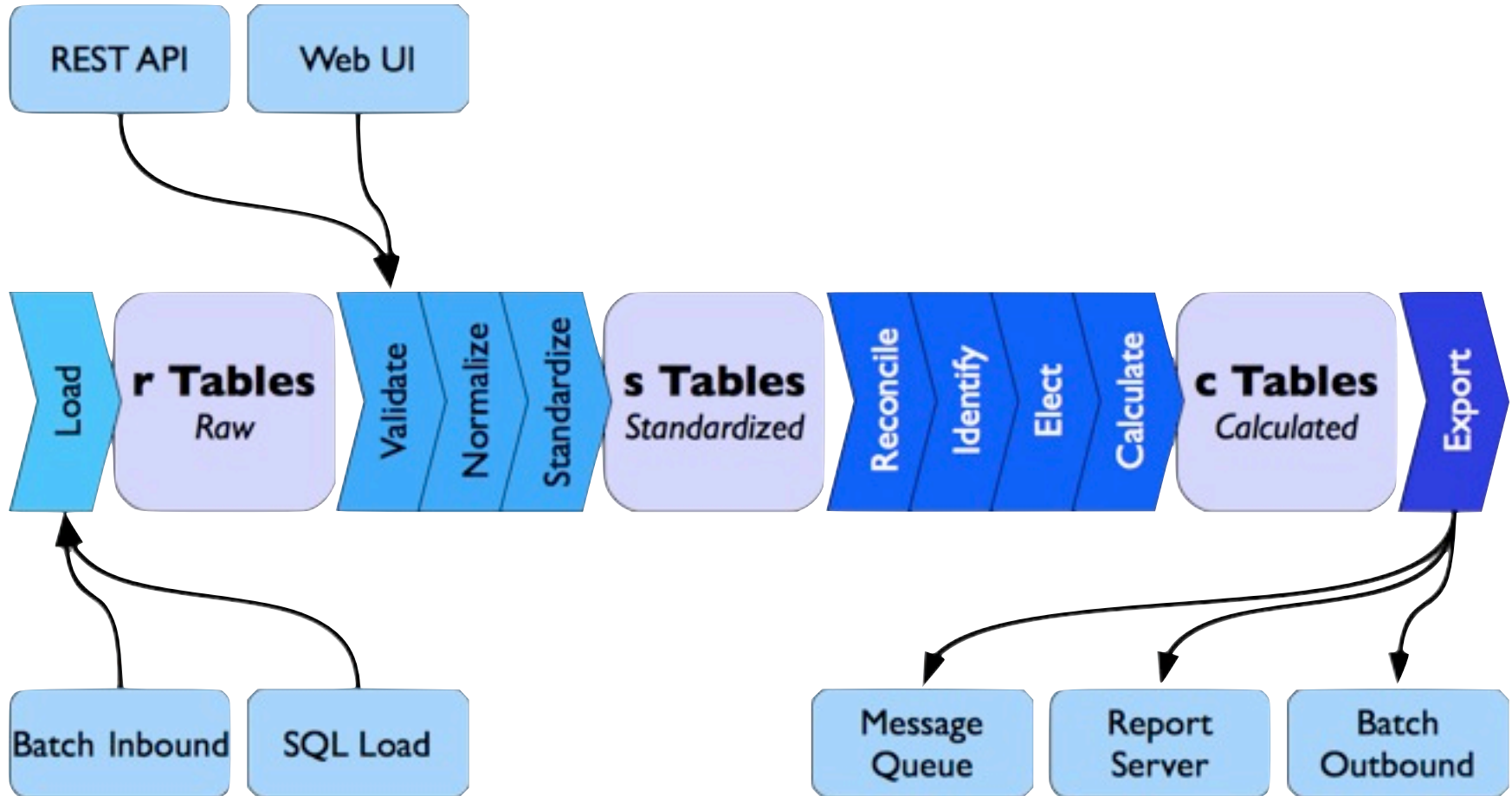
Kipling, Rudyard

Former Undergrad
Staff
Bookstore Clerk



OpenRegistry Architecture

Data Flow, June 2009



Virtual Organizations

- An Organization that consists of members of other Organizations who come together for some purpose
- For example: Researchers from several universities collaborating on a project
- Generally require shared resources
 - Ideally federated
 - Access management handled by the VO
 - Hosted at one Org, at the VO, or in the Cloud
 - Often includes access to instruments, data sets in addition to more common technologies like wikis, mailing lists

Registries: Enterprises vs VOs

Enterprises

- SORs: SIS, HR, Alumni, Guests, etc
- IdPs: Internal, Federated, Social
- Most everything else looks the same
 - Applications
 - Groups/Authorizations
 - Onboarding and termination (lifecycles)

VOs

- SORs: Enterprises (and maybe internal)
- IdPs: Federated, Social

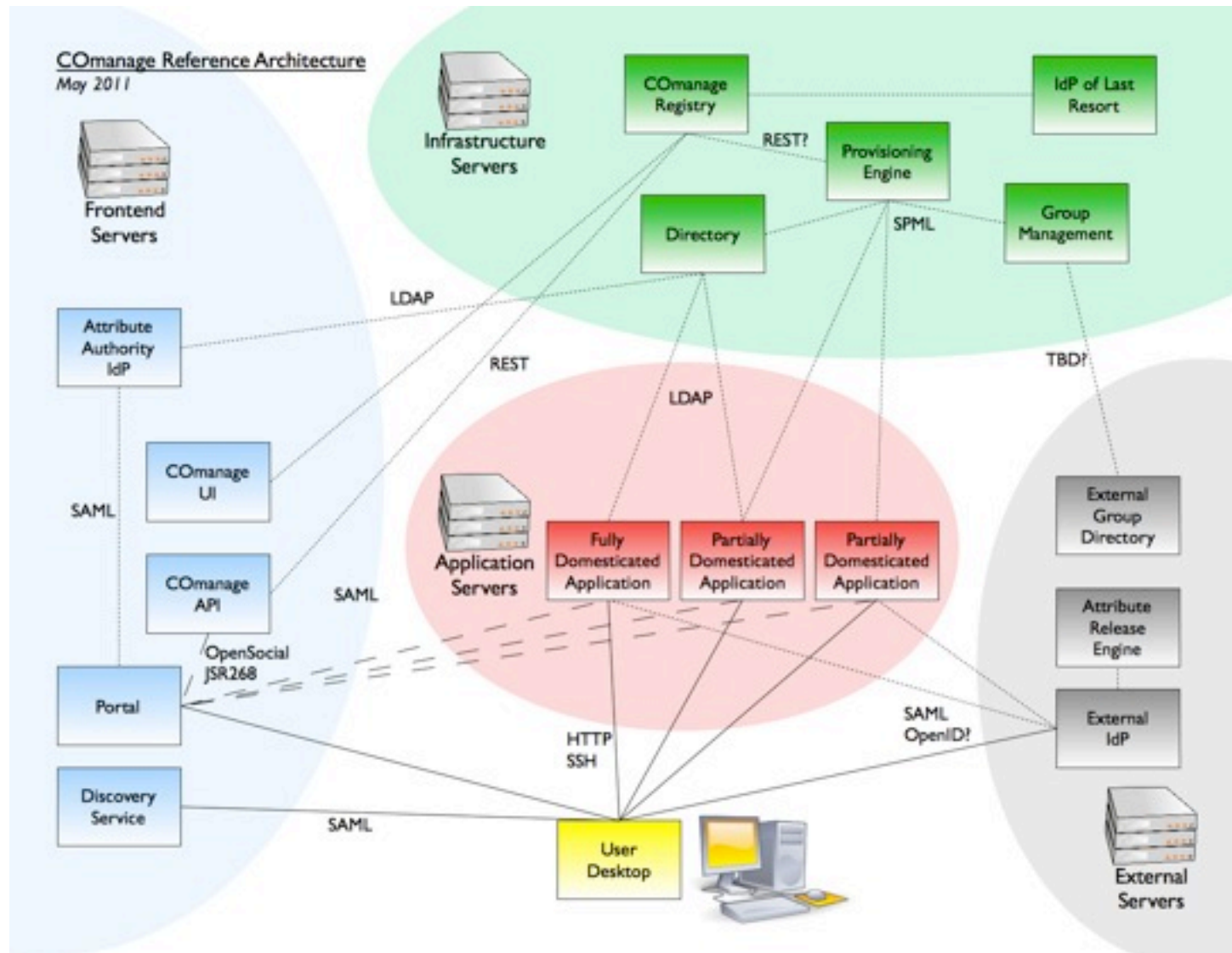
COmanage

- COmanage Registry
 - An Identity Registry for Virtual Organizations
 - Early demo code available
 - Major enhancements on the roadmap
- Collaboration Management Platform
 - An architecture for integration of identity services for Virtual Organizations
 - Registry, Group Management, Permission Management, etc
- A Community of Practice

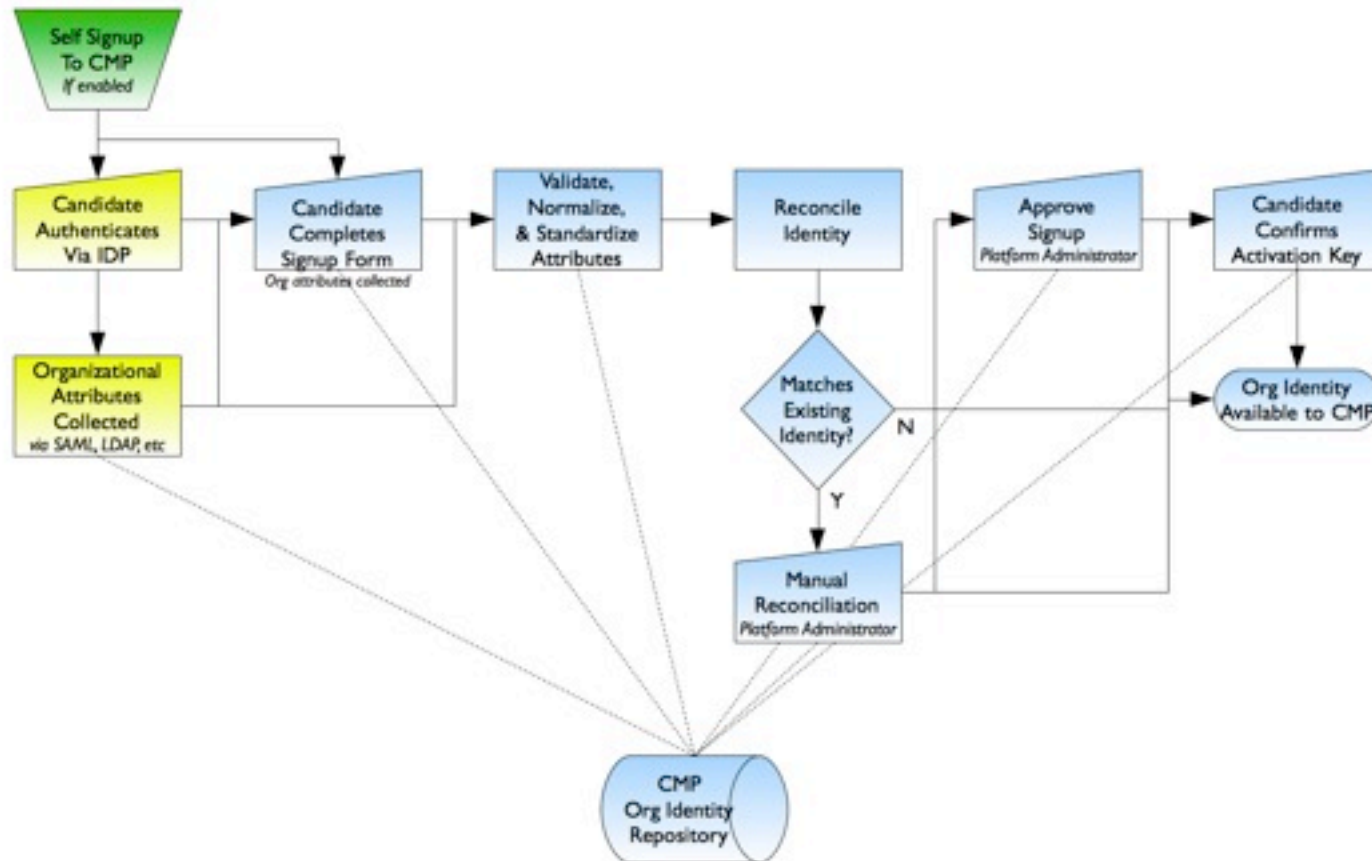
COmanage

- Gathering requirements and developing software in partnership with various Virtual Organizations and other CMPs
 - LIGO
 - Laser Interferometer Gravitational-Wave Observatory
 - Trying to detect gravitational waves
 - iPlant: Cyberinfrastructure collaborative for the plant sciences
 - GENI: Global network engineering
 - Bamboo: Shared infrastructure for humanities research
 - SurfNet: Dutch CMP
 - and others

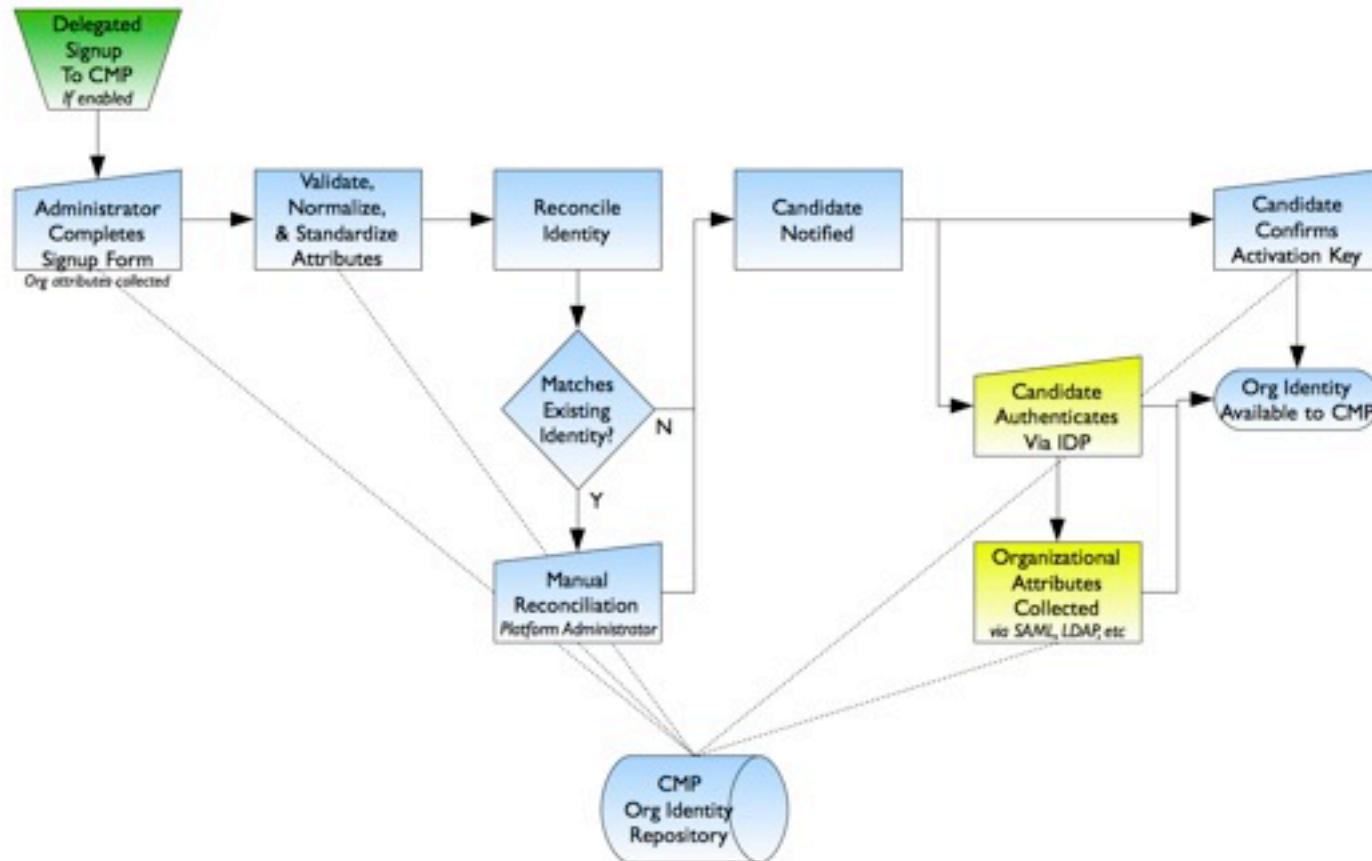
OpenSource Identity Registries



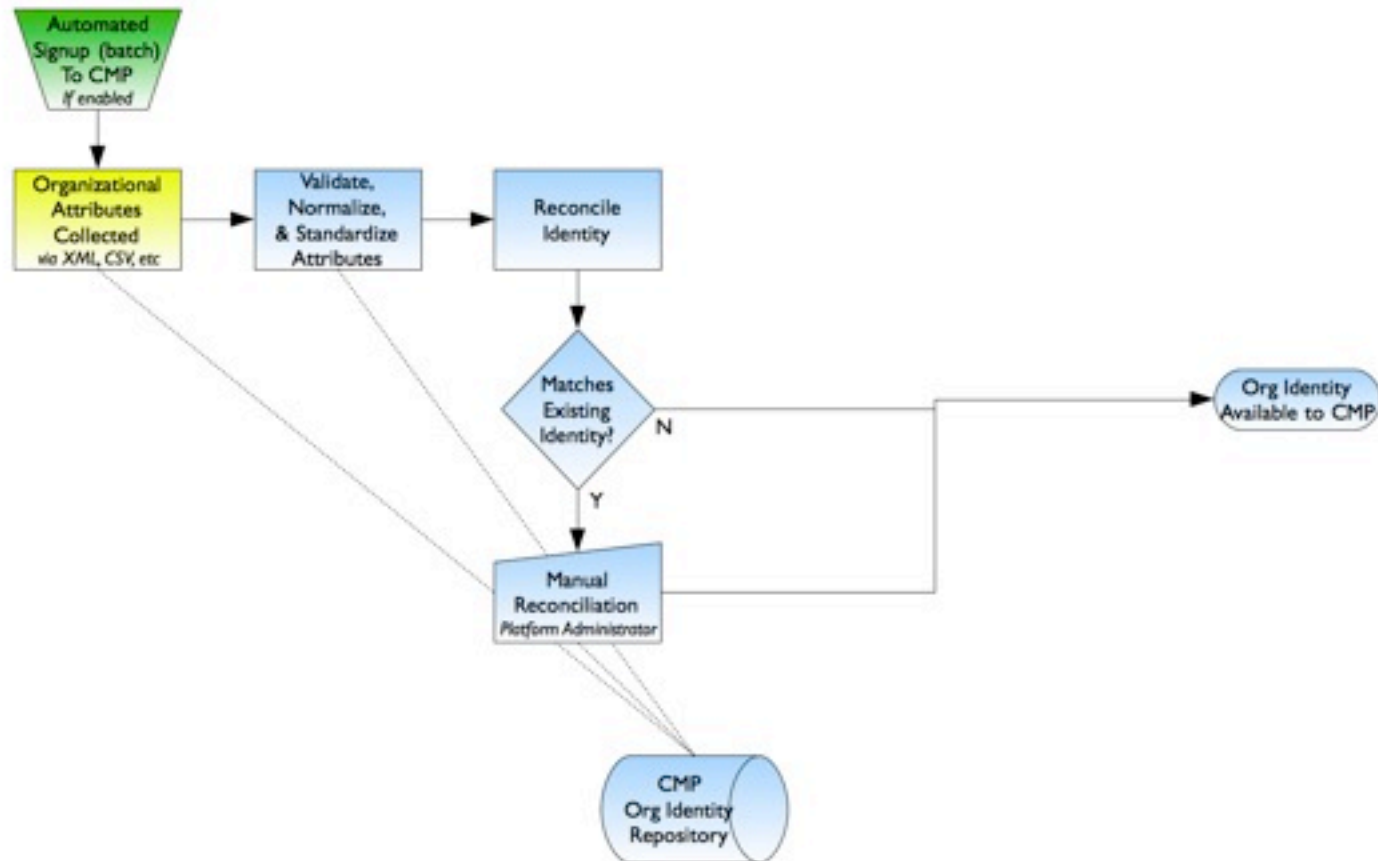
CMP Identity Intake Self Signup, April 2011



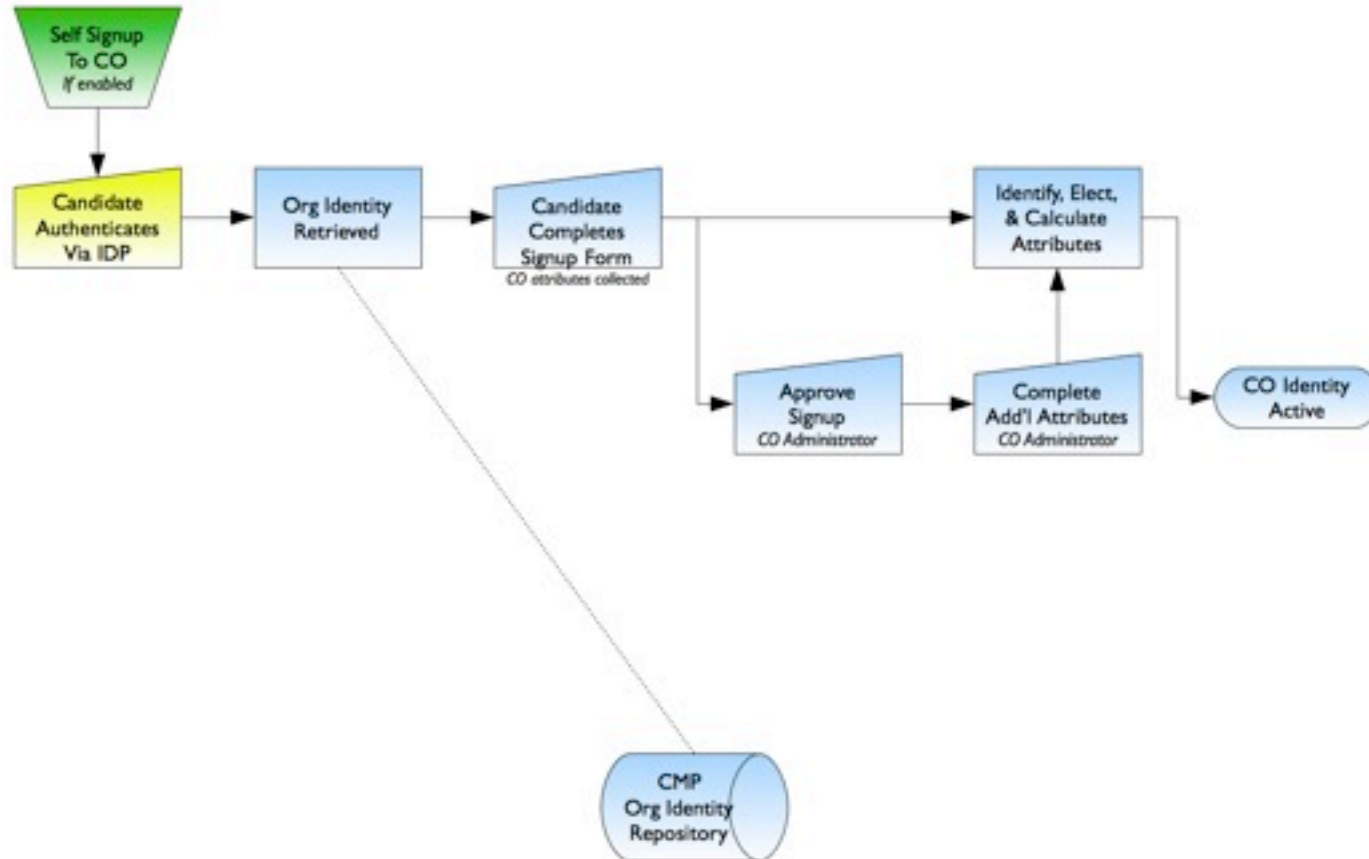
CMP Identity Intake Delegated Signup, April 2011



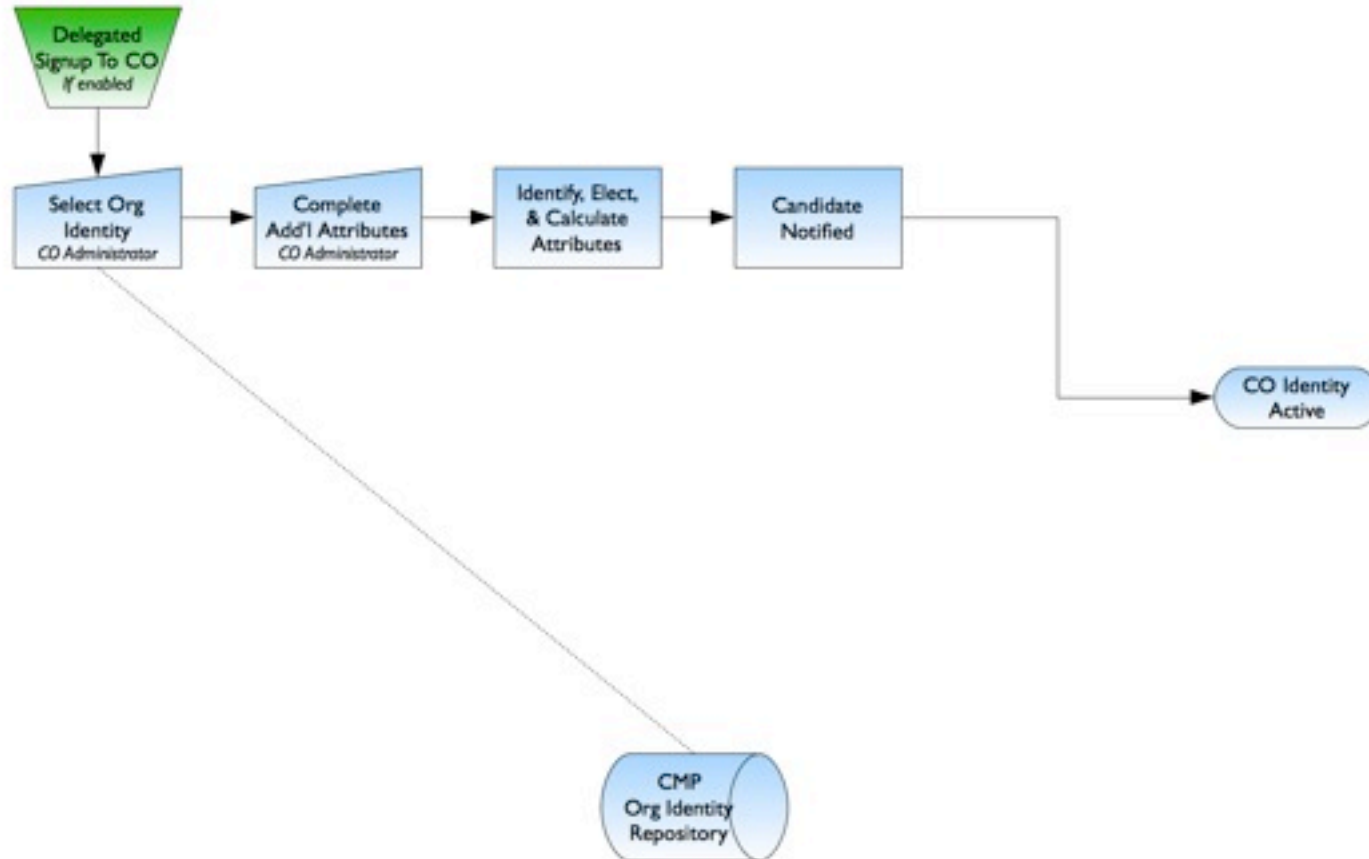
CMP Identity Intake *Automated Signup, April 2011*



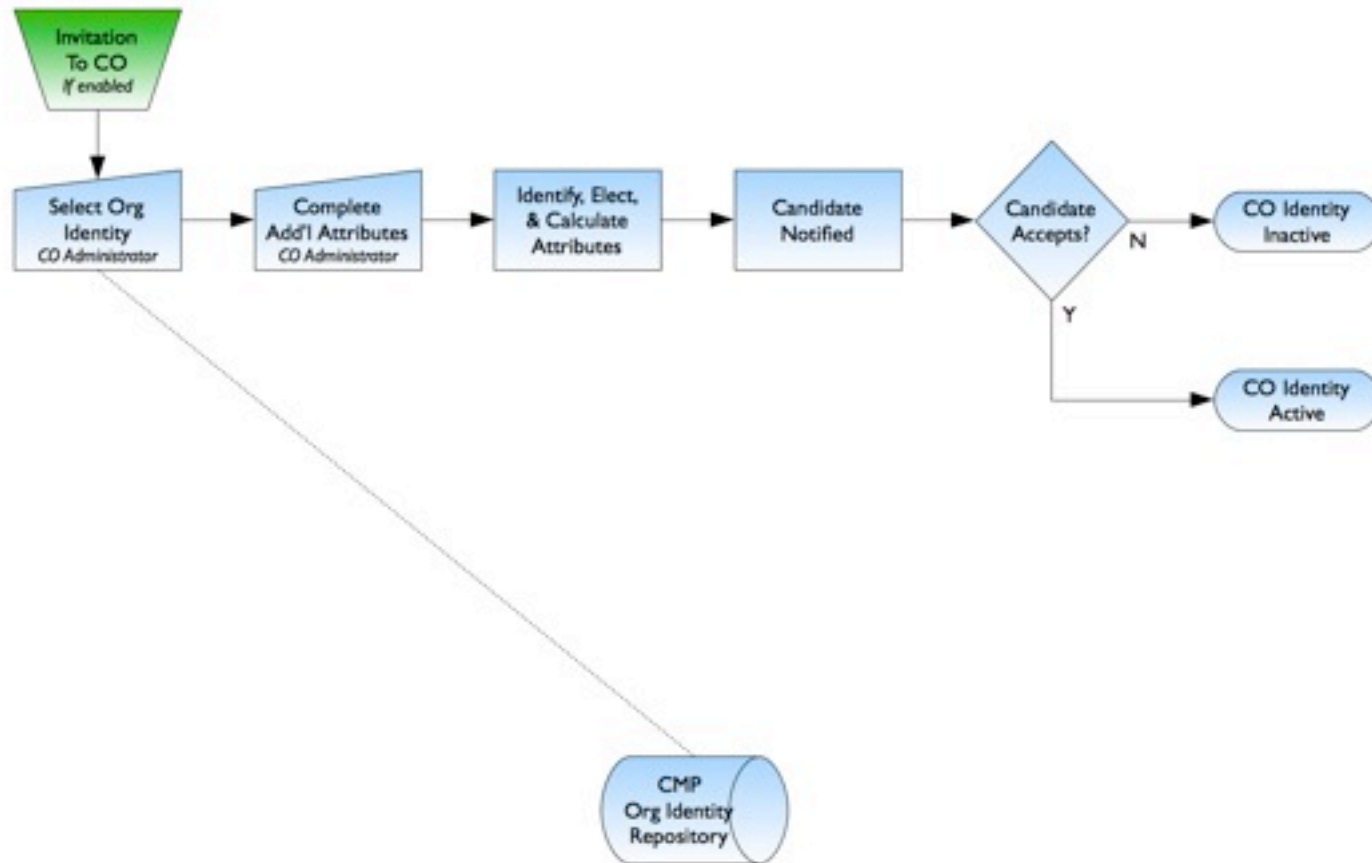
CMP CO Enrollment Self Signup, April 2011



CMP CO Enrollment Delegated Signup, April 2011



CMP CO Enrollment Invite Signup, April 2011



Demo

- Time permitting
- Federated auth
- Provisioning to demo wiki

More Information

- <https://wiki.jasig.org/display/OR>
BoF Monday (today) - 4:45pm - Waverly
Presentation Tuesday - 2:00pm - Cotton Creek 1
- <http://comanage.internet2.edu>
Presentation Tuesday - 11:30am - Cotton Creek 1
Presentation Tuesday - 4:45pm - Cotton Creek 1