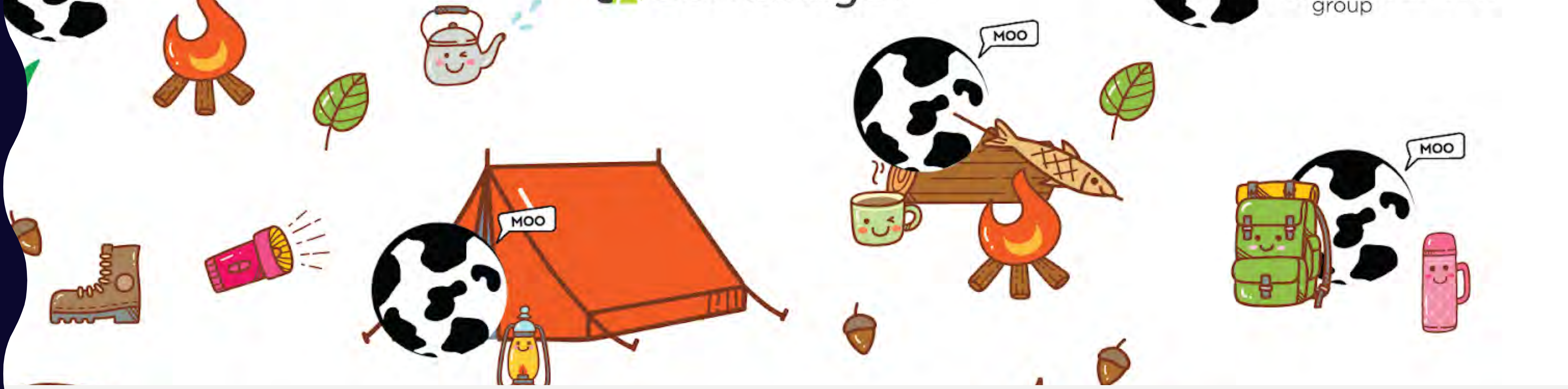


IDENTITY REGISTRATION 201

baseCAMPING WITH THE COW
COMANAGE REGISTRY

InCommon. BaseCAMP

YOUR CAMP COUNSELOR

Laura Paglione serves as an independent consultant with Spherical Cow Group helping technology companies, research institutions and nonprofits develop, implement and market their research infrastructure products. She seeks to inspire organizations to take the road less traveled, embrace alternative solutions, and ditch rigid ideals. She facilitates community engagement for COmanage, coordinates stakeholders of the open-source project, and develops resources for the community including the training materials for COmanage. Laura also serves as the Vice Chair of the InCommon Steering Committee and a member of the Trust and Identity Program Advisory Group. (LauraPaglione.com)

Spherical Cow Group (SCG) was established in 2012 and has been involved with InCommon for over 10 years. Its eight partners work with organization in higher education, research, scholarly communications, standards and NGOs, including virtual organizations. SCG leads the COmanage open-source project and development, designs and teaches its training programs, and works with clients who seek to customize COmanage for their needs. (SphericalCowGroup.com)

MOO

scg

GETTING READY

BACKGROUND: IDENTITY REGISTRIES & COMANAGE

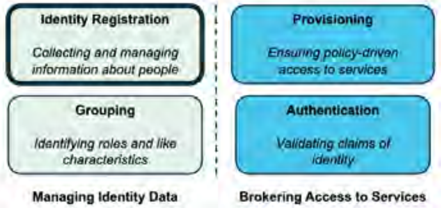
InCommon BaseCAMP

WayBackMachine

Identity Registries and Person Repositories

Concepts to cover:

- Aggregating person data
- Person matching and deduplication
- Repositories (directories, databases, MDM)
- Identity proofing and credentialing


Identity Registration
Collecting and managing information about people
Provisioning
Ensuring policy-driven access to services
Grouping
Identifying roles and like characteristics
Authentication
Validating claims of identity
Managing Identity Data
Brokering Access to Services

IDENTITY REGISTRY & PERSON REPOSITORY

KEY FEATURES

Aggregating person data – Person Registry

- Multiple institutional sources of truth
- Common repositories
- Single person, multiple roles
- Least privilege / additive privilege
- Services based on sum of roles

Person matching & deduplication

- Demographic comparison
- Duplicate detection & remediation

Person repositories

- Database
- Directory
- Application

Identity proofing & assurance

- Assurance levels

COMANAGE IS USED FOR

PERSON LIFECYCLE MANAGEMENT

Enrollment + Lifecycle Actions (changes, offboarding, …)
Enroll and manage individuals into your Identity and Access Management systems in diverse ways

Synthesis
Combine information about a person from different sources (Systems of Record) into a single, comprehensive record

Organization/group Modeling
Model your organization as broad "groups" and attaching this group information to identity records; transfer to LDAP

Basic Provisioning/De-provisioning
Provision information to directly manage access to systems or services, or to manage access via other tools like midPoint or Grouper

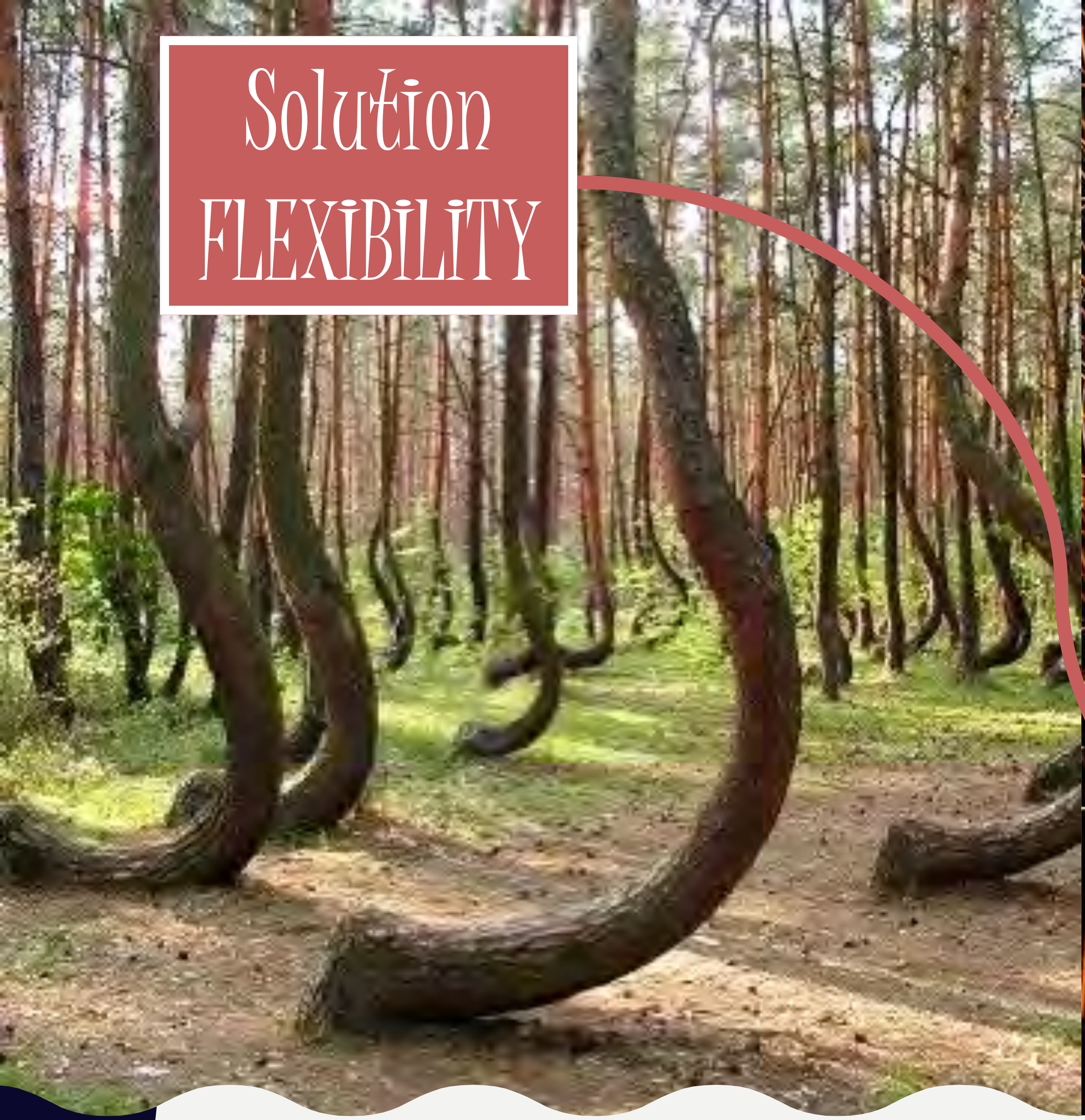
YES, A TOOL… BUT THE DETAILS MATTER FOR IMPLEMENTATION

USE CASE	Research Project / VO	Primary Registry	Guest Registry
People and resource access	Manage people from diverse locations / different authentication; access to limited set of specific resources	Manage home population; sophisticated resource access	Manage a non-primary population (parents, library users, etc); usually no institutional sign in; access to limited resources
Aggregating person data	The same person may participate in multiple projects or hold multiple affiliations	Multiple sources of record for a single person (HR, Student system, affiliate system, etc)	Multiple personas – a guest may hold other roles w/your institution
Person information storage	A simple person registry may be enough	Want information stored in a separate, well-established location (like LDAP)	Want the information separate from primary database to avoid accidental co-mingling
Person lifecycle management	Managed by project rules	Might be handled by HR or student database & rules	
Common solution	Handled by a person registry; light group management & provisioning too	Specialized tools for each component; person registry may be a "helper"	Person registry for lifecycle management; more sophisticated tools too

COMANAGE CAPABILITIES

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

- Onboarding
- Match and Linking
- Identifier
- User Life Cycle
- Provisioning
- Web SSO
- Efficiency



Solution FLEXIBILITY

Implementation COMPLEXITY

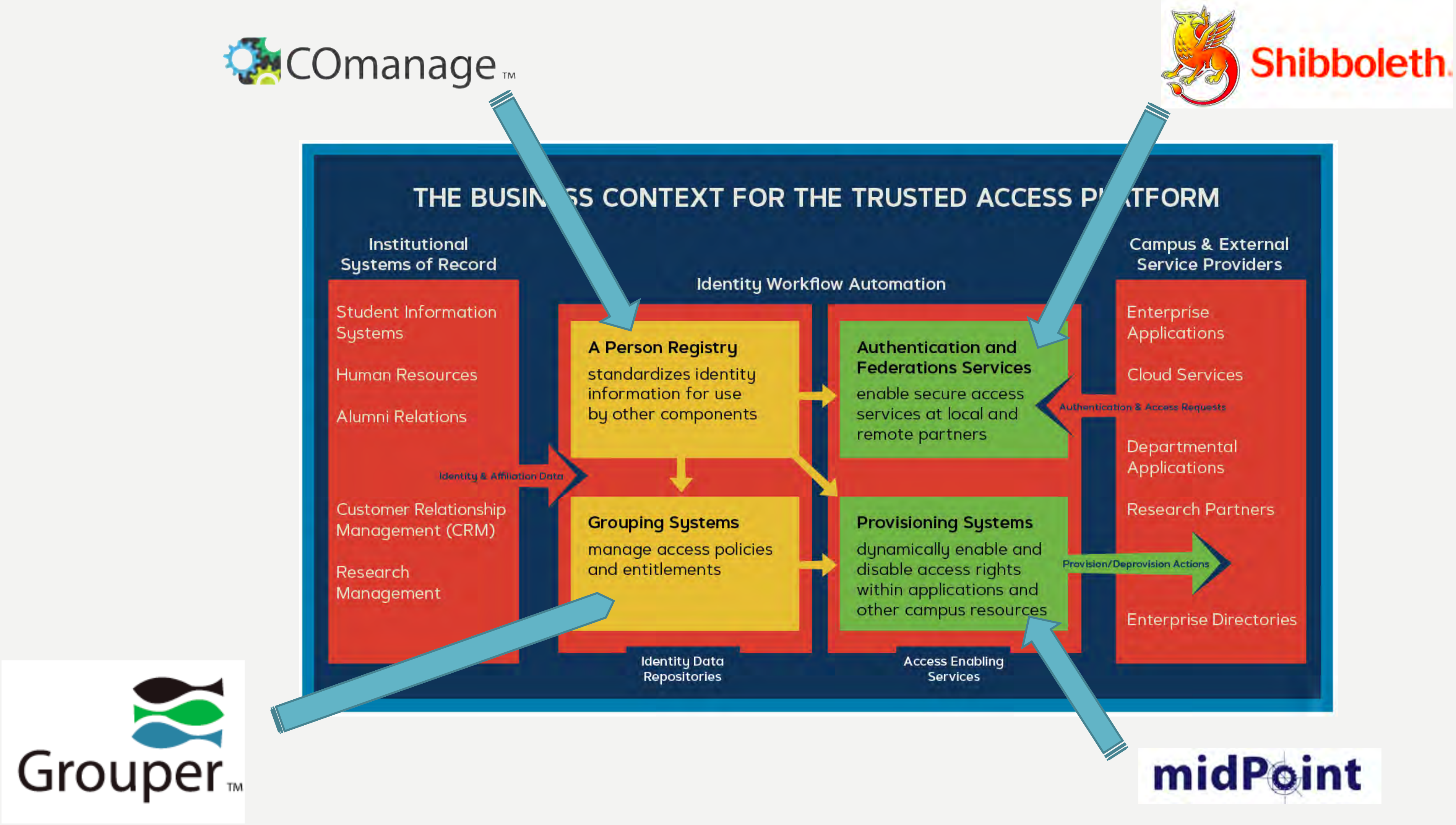
COMANAGE HISTORY

- Open-Source project
  - Project & Development lead: Spherical Cow Group
  - Community directed by the COmanage Program Steering Group (Community Working Group)
  - Code contributions made by the global community
  - Many enhancements are dedicated back to the open-source project to benefit all
- Started in 2010 as a project funded by NSF and Internet2
- Goal to leverage FIM services to support collaborative organizations
- Includes a rich set of APIs and plug-ins that enable connections to other systems

THE CAMPSITE

UNDERSTANDING THE COMANAGE ENVIRONMENT

TAP SOFTWARE CENTERS



COmanage™

Shibboleth

Grouper™

midPoint

THE BUSIN SS CONTEXT FOR THE TRUSTED ACCESS P TFORM

Institutional Systems of Record

- Student Information Systems
- Human Resources
- Alumni Relations
- Customer Relationship Management (CRM)
- Research Management

Identity & Affiliation Data

Identity Workflow Automation

A Person Registry standardizes identity information for use by other components

Grouping Systems manage access policies and entitlements

Identity Data Repositories

Authentication and Federations Services enable secure access services at local and remote partners

Provisioning Systems dynamically enable and disable access rights within applications and other campus resources

Access Enabling Services

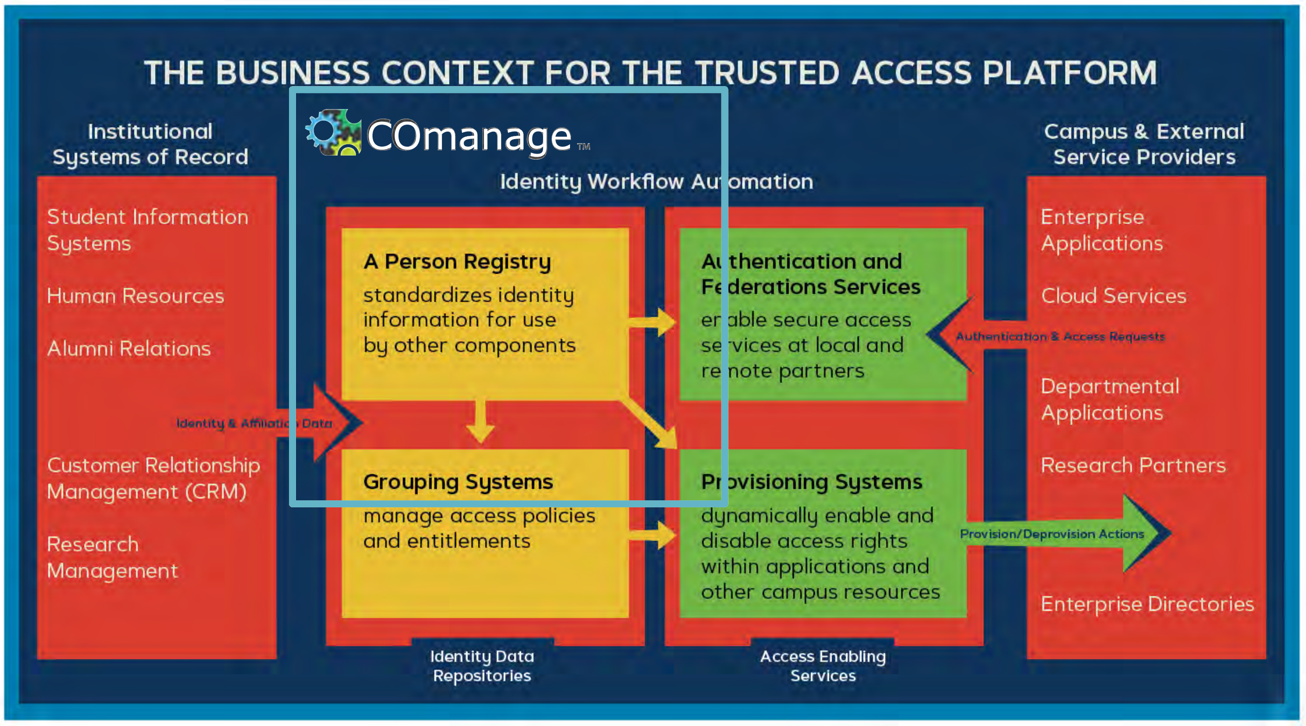
Campus & External Service Providers

- Enterprise Applications
- Cloud Services
- Departmental Applications
- Research Partners
- Enterprise Directories

Authentication & Access Requests

Provision/Deprovision Actions

TRUSTED ACCESS PLATFORM CONTEXT



THE BUSINESS CONTEXT FOR THE TRUSTED ACCESS PLATFORM

COmanage™

Identity Workflow Automation

Institutional Systems of Record

- Student Information Systems
- Human Resources
- Alumni Relations
- Customer Relationship Management (CRM)
- Research Management

A Person Registry
standardizes identity information for use by other components

Grouping Systems
manage access policies and entitlements

Identity Data Repositories

Authentication and Federations Services
enable secure access services at local and remote partners

Provisioning Systems
dynamically enable and disable access rights within applications and other campus resources

Access Enabling Services

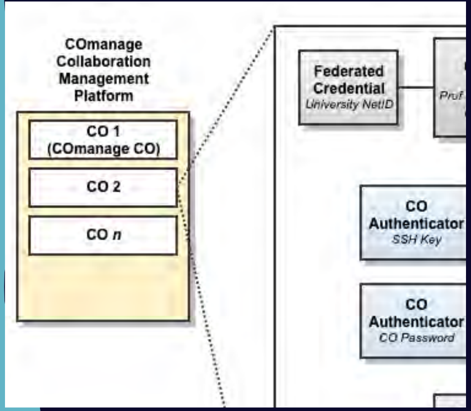
Campus & External Service Providers

- Enterprise Applications
- Cloud Services
- Departmental Applications
- Research Partners
- Enterprise Directories

Identity & Affiliation Data
Authentication & Access Requests
Provision/Deprovision Actions

COMANAGE IS A PERSON REGISTRY… PLUS…

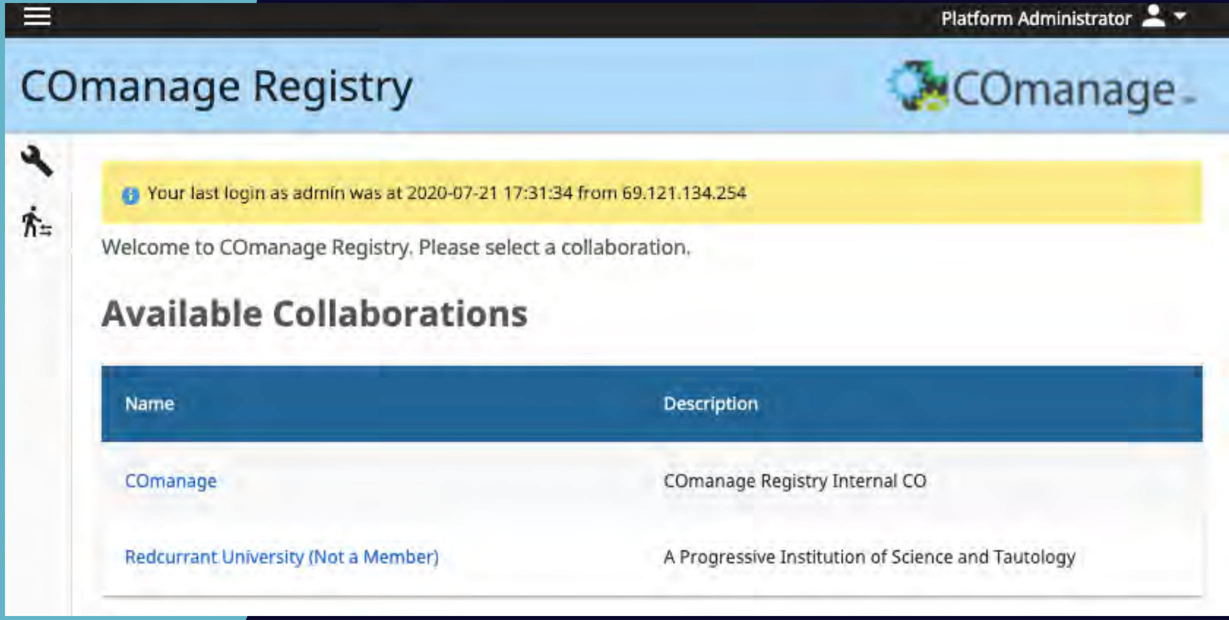
COLLABORATIVE ORGANIZATIONS



- Collaborative Organizations (CO): the main object of COmanage

- A CO is any formal or informal group of individuals working collaboratively in a digital setting

- For each installation of COmanage, one or more top—level Collaborative Organizations (tenants)



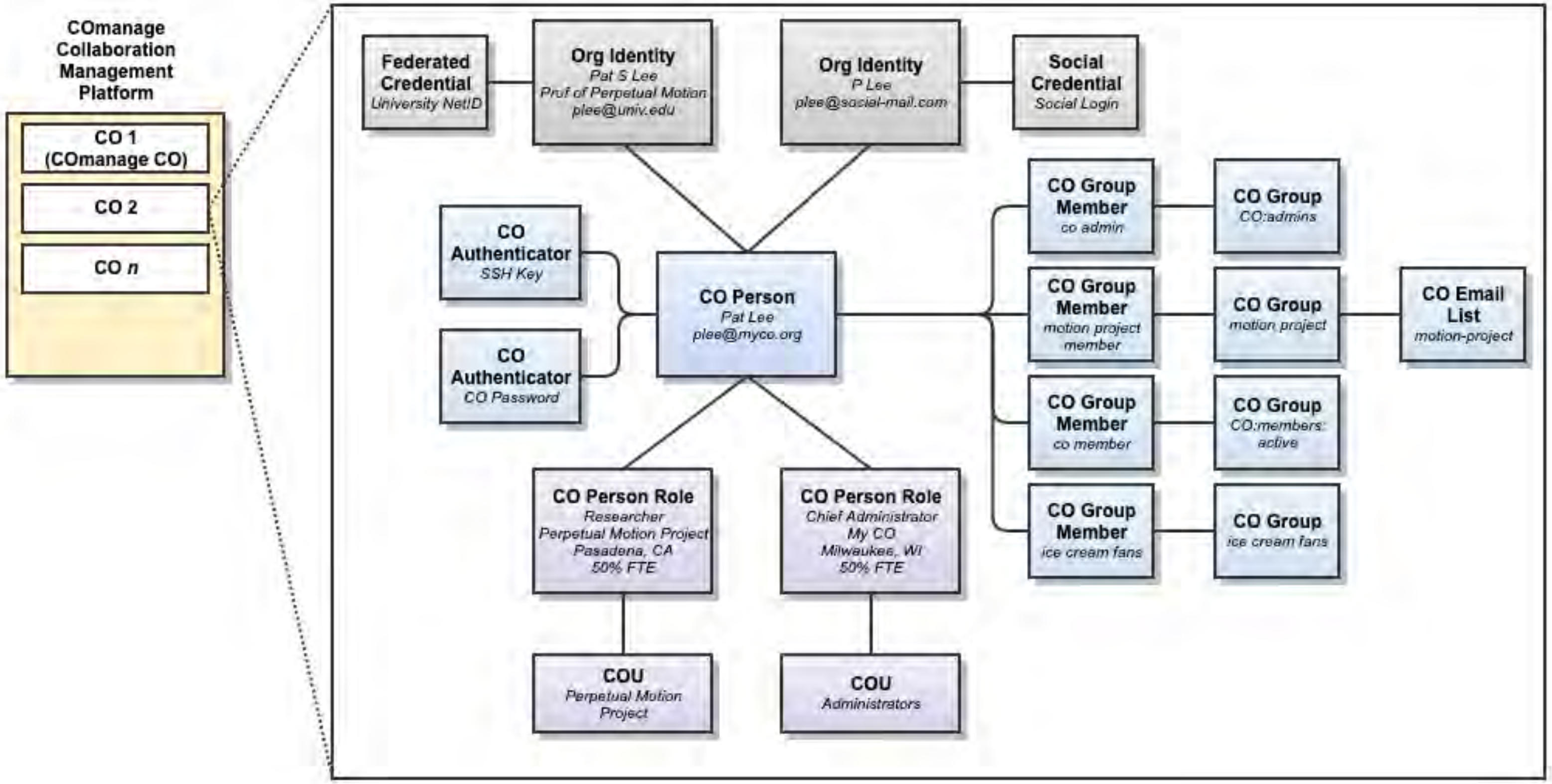
COmanage Registry

Your last login as admin was at 2020-07-21 17:31:34 from 69.121.134.254

Welcome to COmanage Registry. Please select a collaboration.

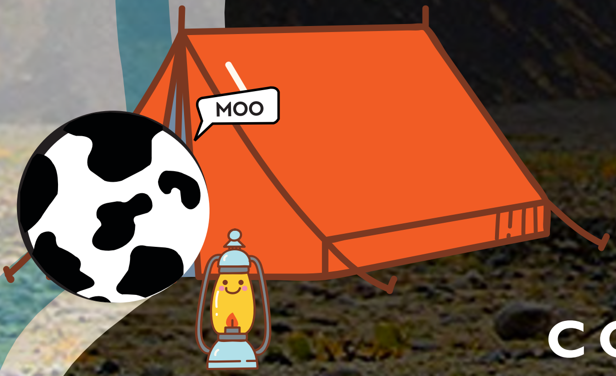
Available Collaborations

Name	Description
COmanage	COmanage Registry Internal CO
Redcurrant University (Not a Member)	A Progressive Institution of Science and Tautology



INSIDE A CO: THE COMANAGE ARCHITECTURE

SETTING UP THE TENT



CONFIGURING COMANAGE

COMANAGE CONCEPTS

PEOPLE

COmanage is a registry for people. People are modeled through the information stored about them from other systems, their roles in organization structures, their memberships in groups, and how they authenticate.

STRUCTURE & ROLES

How the people naturally fall into groups, perhaps by organizational unit, project team or the activities that a group of people can do. Comanage has several structures to model your Collaborative Organization.

EXTERNAL SYSTEM LINKS

COmanage is particularly good at linking stored people to their representations in other systems. These systems include “inbound systems” that provide information to Comanage, as well as “outbound systems” that enables provisioning this collected information.

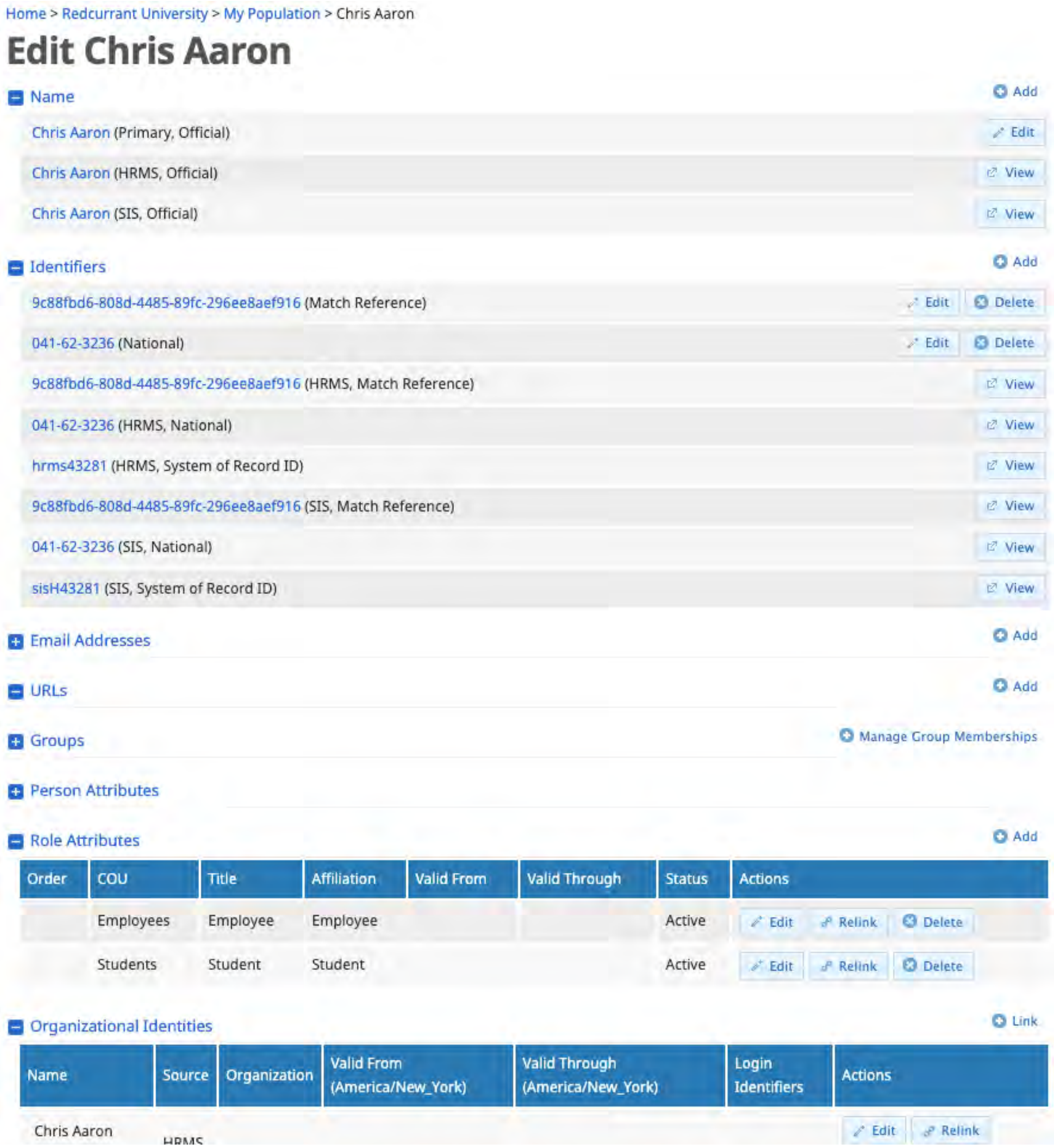
ENROLLMENT FLOWS

Extremely powerful and flexible workflows to import, create, configure, and manage people in COmanage and share this information with other systems.

MODELING PEOPLE

CO Person
the representation of a person in COmanage

- **Identifiers** – unique identifiers representing individuals in COmanage & elsewhere
- **CO Person Role** – the roles the individual plays in the CO
- **Org Identity** – stores attributes about the person
  - Often from an external system (System of Record)
  - Includes attributes from Systems of Record
  - Can include an authenticator for sign in



Home > Redcurrant University > My Population > Chris Aaron

Edit Chris Aaron

Name

Chris Aaron (Primary, Official)

Chris Aaron (HRMS, Official)

Chris Aaron (SIS, Official)

Identifiers

9c88fbd6-808d-4485-89fc-296ee8aef916 (Match Reference)

041-62-3236 (National)

9c88fbd6-808d-4485-89fc-296ee8aef916 (HRMS, Match Reference)

041-62-3236 (HRMS, National)

hrms43281 (HRMS, System of Record ID)

9c88fbd6-808d-4485-89fc-296ee8aef916 (SIS, Match Reference)

041-62-3236 (SIS, National)

sisH43281 (SIS, System of Record ID)

Email Addresses

URLs

Groups

Person Attributes

Role Attributes

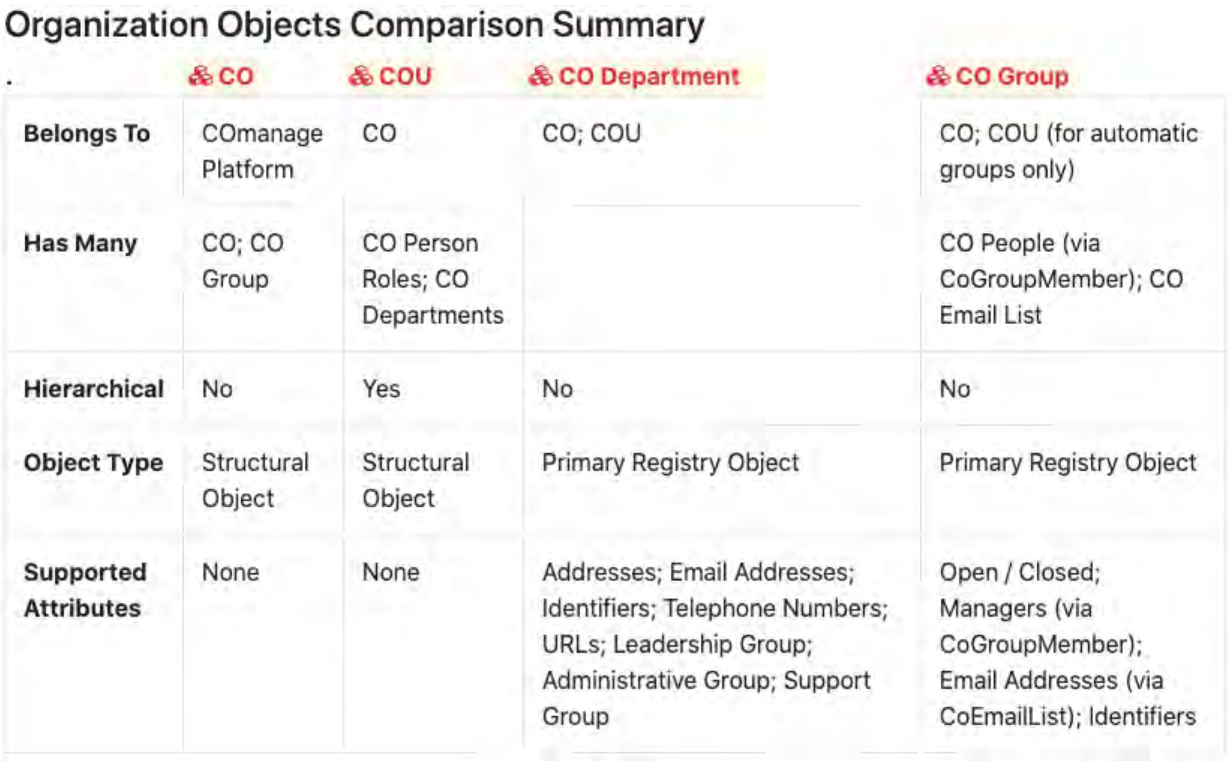
Order	COU	Title	Affiliation	Valid From	Valid Through	Status	Actions
	Employees	Employee	Employee			Active	Edit Relink Delete
	Students	Student	Student			Active	Edit Relink Delete

Organizational Identities

Name	Source	Organization	Valid From (America/New_York)	Valid Through (America/New_York)	Login Identifiers	Actions
Chris Aaron	HRMS					Edit Relink

MODELING ORGANIZATIONS

- **CO** – Collaborative Organization
- **COU** – CO Unit
  the structural sub-units of the CO
- **CO Group** – flexible groups
  can be open or closed; can support distributed management
- **CO Department** –
  store information useful for describing parts of the organization



Organization Objects Comparison Summary

.	CO	COU	CO Department	CO Group
Belongs To	COmanage Platform	CO	CO; COU	CO; COU (for automatic groups only)
Has Many	CO; CO Group	CO Person Roles; CO Departments		CO People (via CoGroupMember); CO Email List
Hierarchical	No	Yes	No	No
Object Type	Structural Object	Structural Object	Primary Registry Object	Primary Registry Object
Supported Attributes	None	None	Addresses; Email Addresses; Identifiers; Telephone Numbers; URLs; Leadership Group; Administrative Group; Support Group	Open / Closed; Managers (via CoGroupMember); Email Addresses (via CoEmailList); Identifiers

EXTERNAL SYSTEM LINKS

Incoming: Systems of Record

PROVIDE

- Attributes
- Identifiers

ENABLE

- Sign in via other tools
- Identity matching & linking

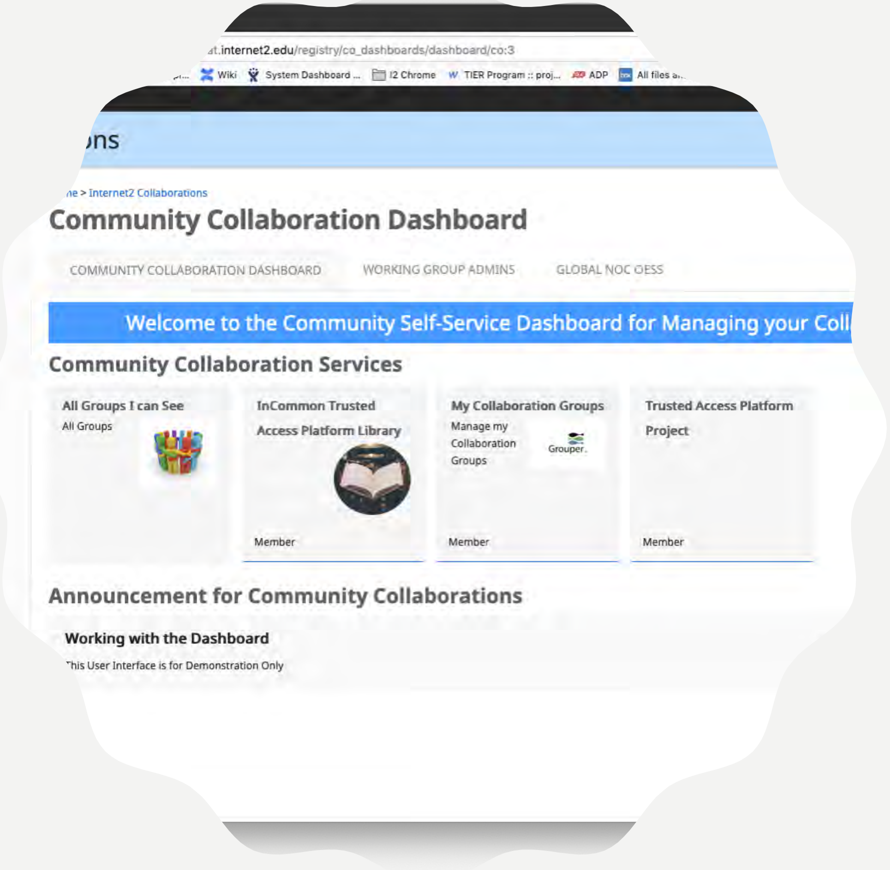
Outgoing: Provisioned Services

PROVIDE

- Attributes to enable system use
- Managed provisioning & deprovisioning based on business rules
- Provisioning to Grouper and other systems for more sophisticated group management

ENABLE

- Real-time checking of incoming system attributes
- Dashboard UI for quick access from COmanage



Community Collaboration Dashboard

Welcome to the Community Self-Service Dashboard for Managing your Coll

Community Collaboration Services

All Groups I can See
All Groups

InCommon Trusted Access Platform Library
Member

My Collaboration Groups
Manage my Collaboration Groups
Member

Trusted Access Platform Project
Member

Announcement for Community Collaborations

Working with the Dashboard

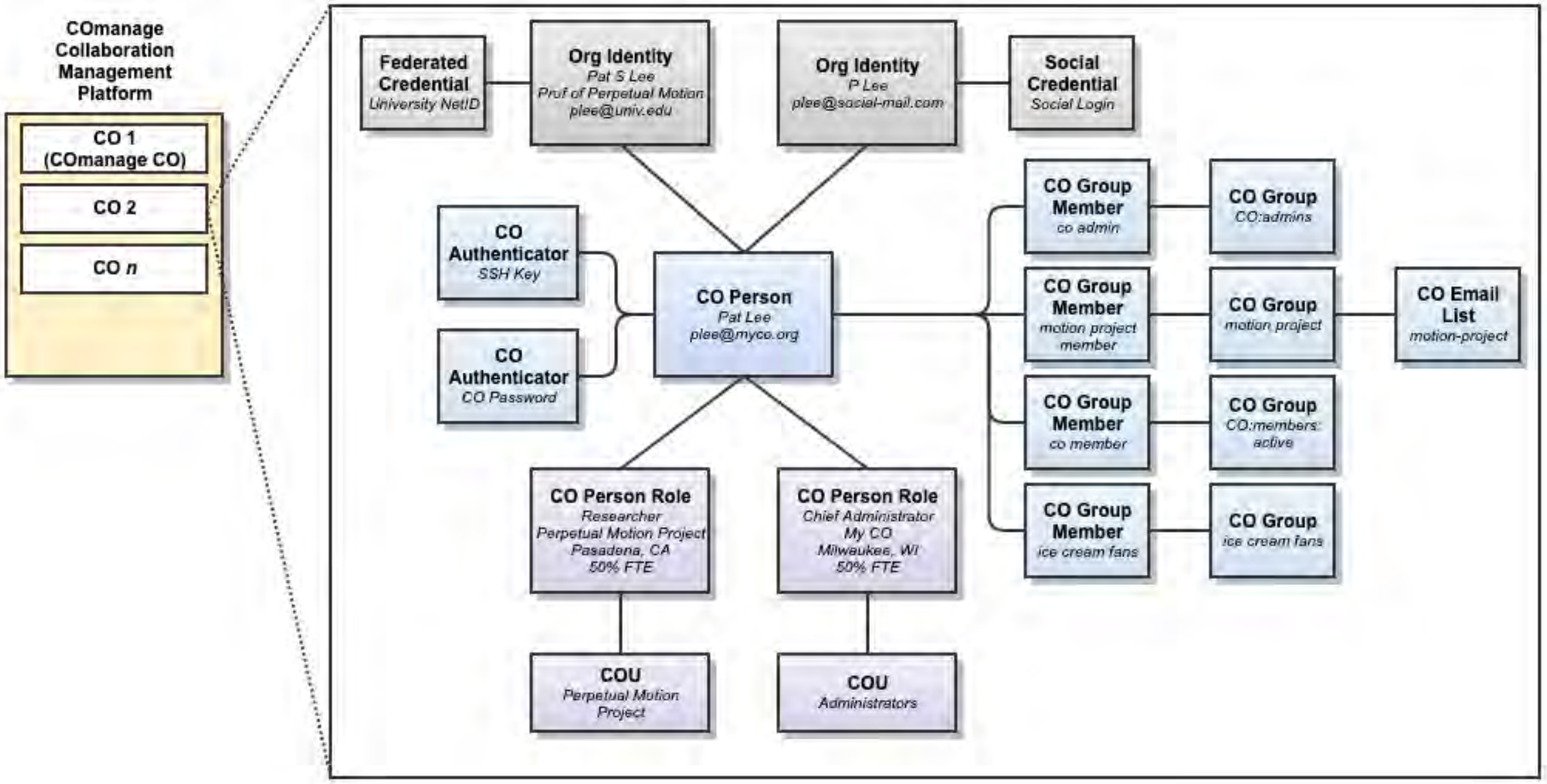
This User Interface is for Demonstration Only

ENROLLMENT WORKFLOW FEATURES

Register	Register individuals to connect to digital tools and resources
Match	Perform identity matching to prevent duplicates
Add	Add individuals to COUs, and CO Groups
Approve	Trigger approval steps as needed
Link	Link to external sources, using attributes to pre-populate information about the individual
Identifiers	Associate internal and external identifiers with the person
Review	Have the individual authenticate to gain access to privileges, verify email addresses, accept terms and conditions
Provision	Provision access to tools, systems and resources
Communicate	Send communications to the individual and others about the enrollment

OTHER WORKFLOWS

- Add a role
- Identity linking
- Setting grace periods (for loss of privileges/access)
- Off boarding



COmanage Collaboration Management Platform

CO 1 (COmanage CO)

CO 2

CO *n*

Federated Credential *University NetID*

Org Identity *Pat S Lee* *Prof of Perpetual Motion* *plee@univ.edu*

Org Identity *P Lee* *plee@social-mail.com*

Social Credential *Social Login*

CO Authenticator *SSH Key*

CO Authenticator *CO Password*

CO Person *Pat Lee* *plee@myco.org*

CO Group Member *co admin*

CO Group *CO:admins*

CO Group Member *motion project member*

CO Group *motion project*

CO Email List *motion-project*

CO Group Member *co member*

CO Group *CO:members:active*

CO Group Member *ice cream fans*

CO Group *ice cream fans*

CO Person Role *Researcher* *Perpetual Motion Project* *Pasadena, CA* *50% FTE*

CO Person Role *Chief Administrator* *My CO* *Milwaukee, WI* *50% FTE*

COU *Perpetual Motion Project*

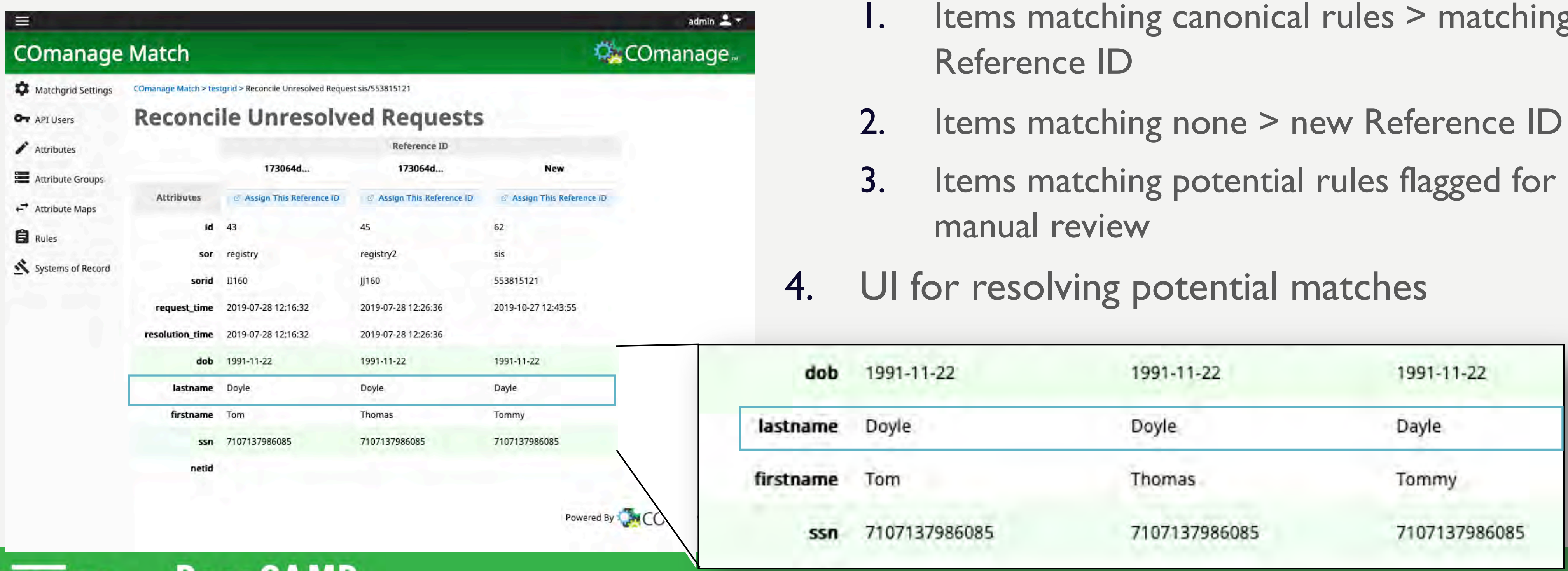
COU *Administrators*

INSIDE A CO: THE COMANAGE ARCHITECTURE

COMANAGE MATCH

- System for matching items
- Use directly in COmanage - match people as they are registered
- API to integrate with other systems

1. Define the attributes to be used for matching
2. Set up rules for matching (Canonical and Potential)
3. As items are evaluated, the rules are checked
   1. Items matching canonical rules > matching Reference ID
   2. Items matching none > new Reference ID
   3. Items matching potential rules flagged for manual review
4. UI for resolving potential matches



COmanage Match > testgrid > Reconcile Unresolved Request sis/553815121

Reconcile Unresolved Requests

	Reference ID		
	173064d...	173064d...	New
Attributes	Assign This Reference ID	Assign This Reference ID	Assign This Reference ID
id	43	45	62
sor	registry	registry2	sis
sorid	II160	JJ160	553815121
request_time	2019-07-28 12:16:32	2019-07-28 12:26:36	2019-10-27 12:43:55
resolution_time	2019-07-28 12:16:32	2019-07-28 12:26:36	
dob	1991-11-22	1991-11-22	1991-11-22
lastname	Doyle	Doyle	Dayle
firstname	Tom	Thomas	Tommy
ssn	7107137986085	7107137986085	7107137986085
netid			

dob	1991-11-22	1991-11-22	1991-11-22
lastname	Doyle	Doyle	Dayle
firstname	Tom	Thomas	Tommy
ssn	7107137986085	7107137986085	7107137986085

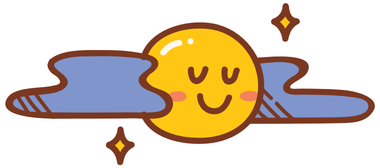
WRAPPING UP THE DAY

WHAT YOU CAN LOOK FORWARD TO

THE SUN IS SETTING, BUT THERE IS SO MUCH MORE…

- Offboarding workflows
- User Interface customization
- Fun with plugins!
- Duplicate management with COmanage Match
- Extending the COmanage data model

TO LEARN MORE



COmanage software page

www.incommon.org/software/comanage/

COmanage training page

www.incommon.org/academy/comanage/

Video by Vladimir Maric from Pixabay

IDENTITY REGISTRATION 201