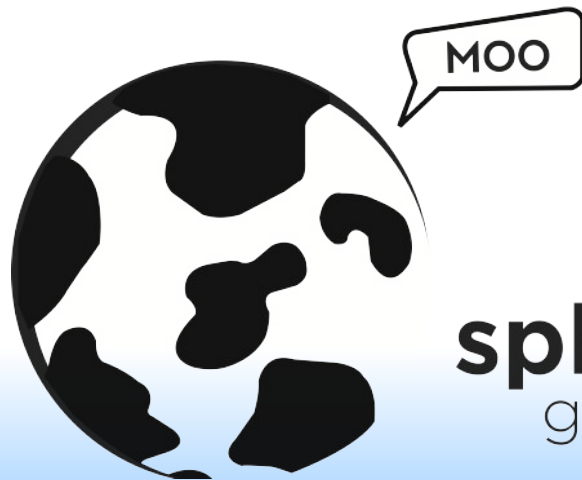# COmanage:
An Introduction

Benjamin Oshrin
January 2018 • Campus Success

spherical cow
group

What Is COmanage [Registry]?

- **COmanage**™ Is The **Project**
- Registry Is The **Product**
  - *(Like "Shibboleth" and "IdP")*
  - A Person* Registry: A place to store information about people associated with your organization
    - *also groups, departments, email lists, services, authenticators, and some other things*
  - Enrollment, Lifecycle, and Attribute Management
  - Complex representations of people with multiple components to their identity

COmanage History

- Originally funded by NSF / Internet2 for Virtual Organizations (obLIGO)
  - *Turns out, VO Identity needs are similar to Institutional Identity needs*
- As adoption grows, contributions are too (financial, patches, bug reports, etc)
  - CILogon (NSF), CTSC (Indiana University), GÉANT, Lafayette, MLA (Mellon), NIH/NIAID (NETE), SUNET, SURFnet, etc
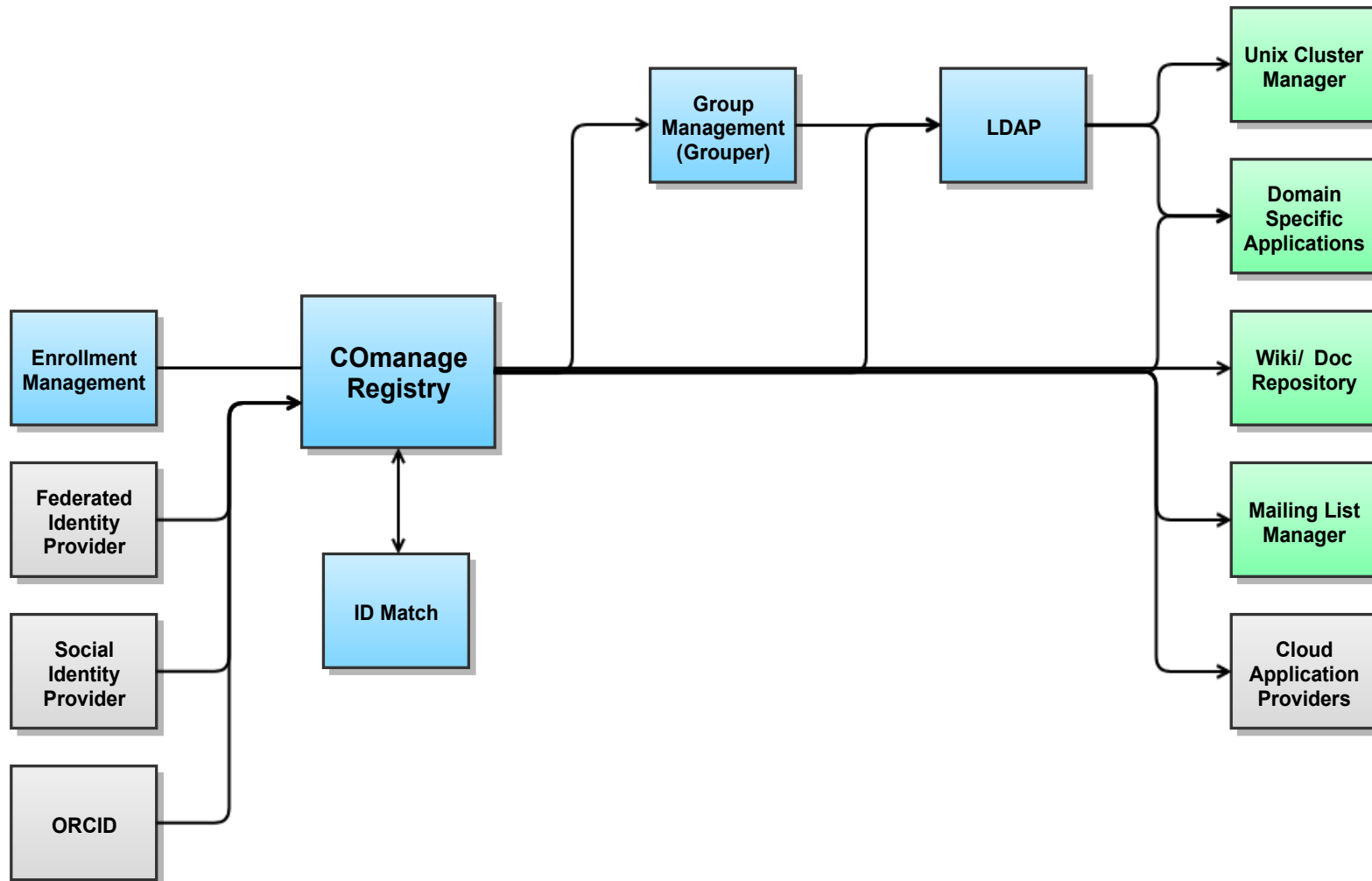
MOO

SC○

What Can You Do With COmanage Registry?

- Virtual Organization / Collaboration Management

- Guest / Non-Traditional Population Management

- University Identity Registry

Some Integration Work May Be Required

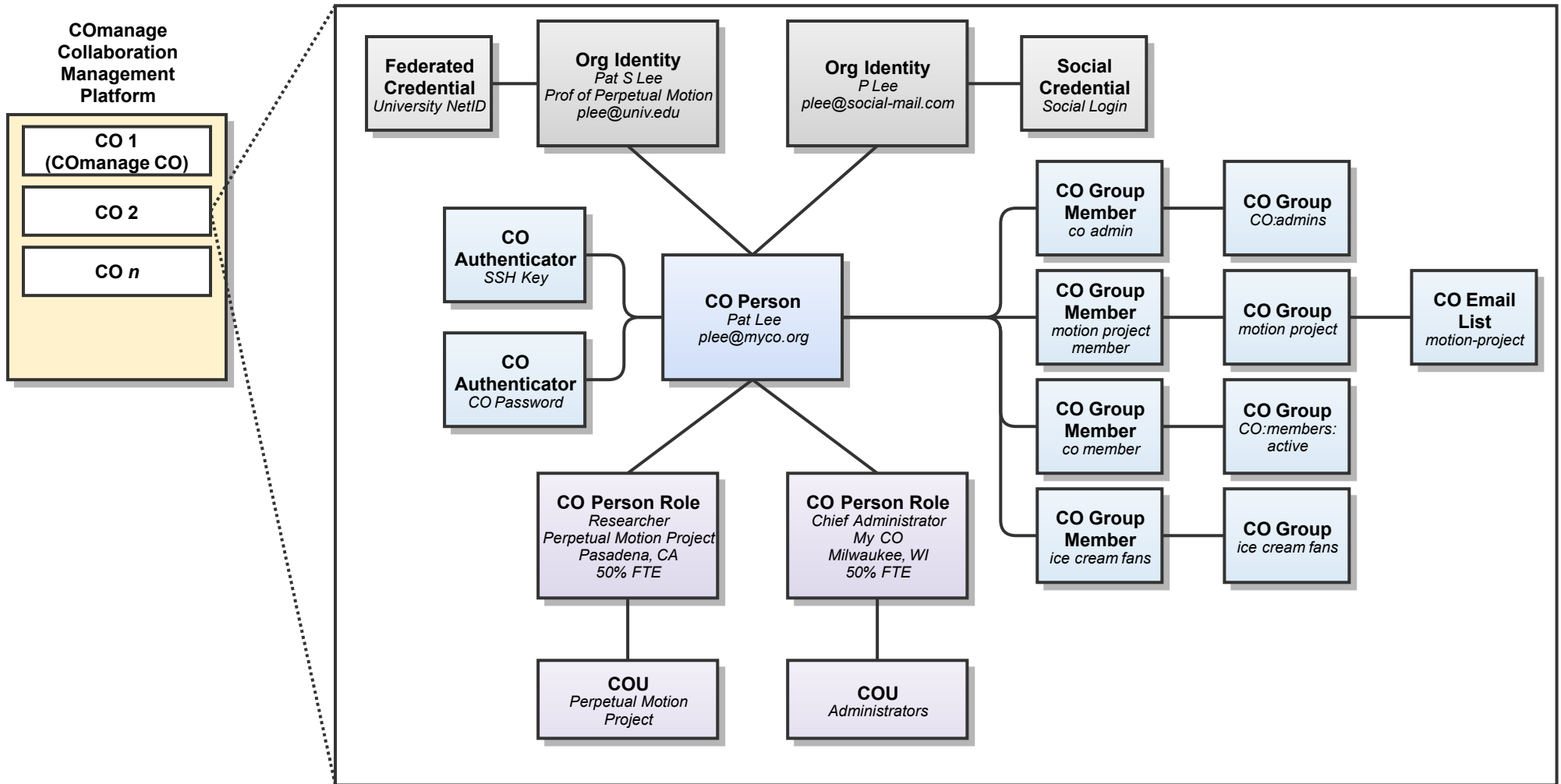# Institutional Component Architecture
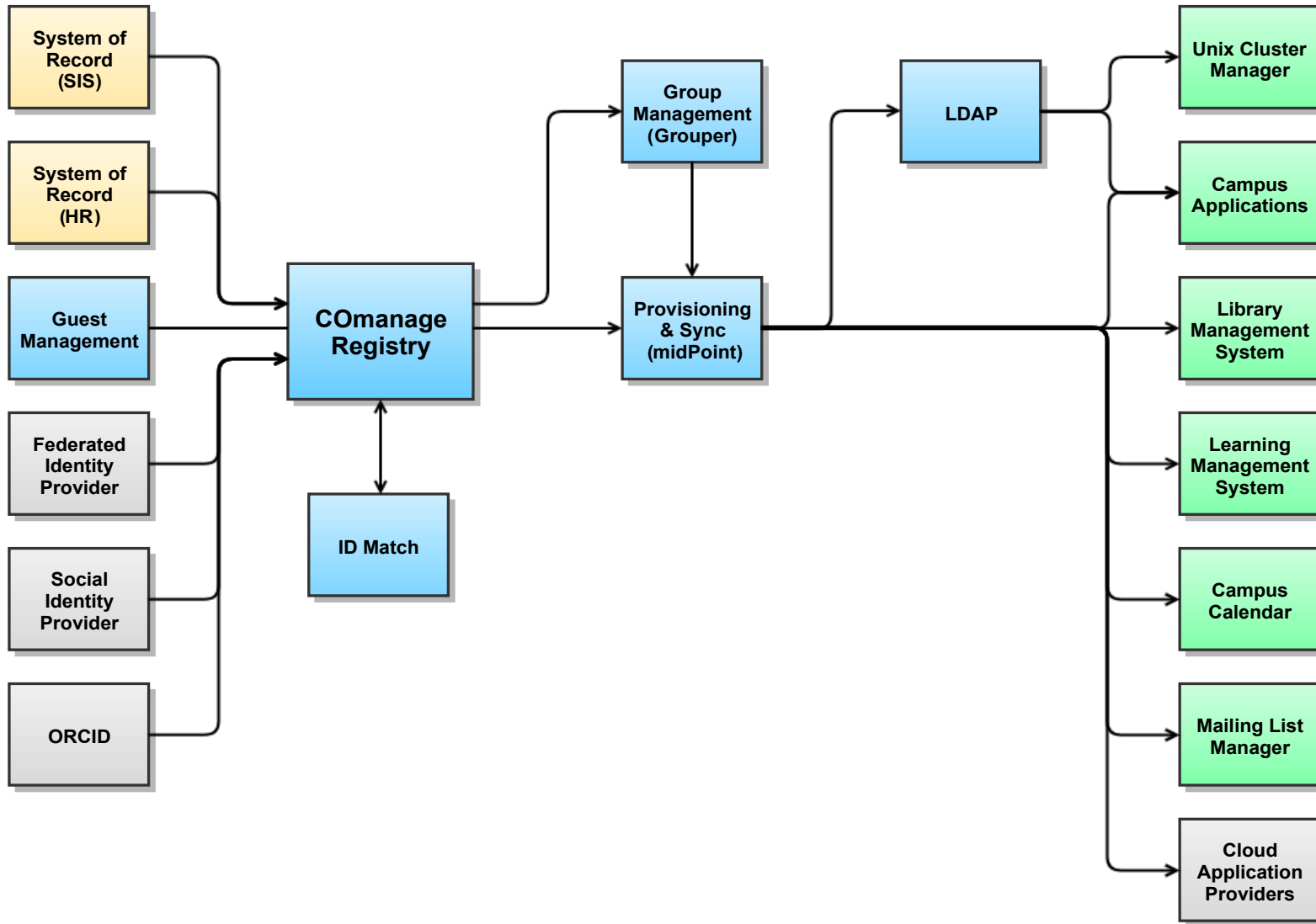
VO Component Architecture

Registry Person Model

Registry Capabilities

- Most non-core features are designed to provide common capabilities out of the box, but allow replacement or integration with more comprehensive products, eg:

  - Group Management → Grouper

  - Provisioning → (eg) midPoint

- UI driven configuration and operation

- REST API

Registry Capabilities

- Person & Role Attribute Management
  - Normalization
  - Attribute Enumerations
  - Multi-valued Names, Addresses, Email Addresses, etc
- Identifier Assignment and Management
  - Pattern based sequential or random identifier assignment
  - Tracking of external (non-Registry) identifiers
- Population Organization
  - COUs & Departments
  - Basic Group Management

MOO

SC

Registry Capabilities

- Self Service & Delegated Enrollment & Lifecycle Management
  - Enrollment Flows
  - Early Onboarding
  - Duplicate Management / Relinking
  - Sponsors
  - Expiration Policies
  - Basic Matching *more to come*
  - Terms & Conditions
- Human Readable Transaction History
  - Person / Group / Email List / Petition
- Database Level "Changelog" (Copy-On-Write)

MOO

SCG

Registry Capabilities: Organizational Identity Sources

- Plugin based mechanism for creating records from external sources

  - Env

  - File

  - LDAP

  - NetFORUM

  - ORCID

  - Salesforce

  - ...

Registry Capabilities: Provisioners

- Plugin based mechanism to provision directly to supported services

  - Changelog

  - GitHub

  - Grouper

  - LDAP

  - Mailman

  - MediaWiki

  - Salesforce *in development*

- Or link up to message bus or provisioning system

Registry Capabilities: Authenticators

- Plugin based mechanism for credential management

  - SSH Keys*

  - Service Tokens*

    – *Existing implementation is not yet plugin based

  - Certificates

  - Passwords

- Current implementation is "beta"

Registry Extensibility & Customization

- Plugins
  - Authenticator
  - Enrollment Flow
  - Identifier Validation
  - Invitation Confirmer
  - LDAP Schema
  - Normalization
  - Organizational Identity Source
  - Provisioner
  - Generic

MOO

SC

Registry Extensibility & Customization

- Extended Attributes

- Extended Types

  - eg: eduPersonAffiliation ↔ localPersonAffiliation

- UI Themes

- I18n and L10n

MOO

SC9

But... does it *scale*?

- Short Answer: Yes, to University scale
- Largest known production deployment O(10k)
- Largest known test deployment O(500k)
- Some rough edges still need smoothing

Product Roadmap

- Registry v3.1.0 at RC2, final release any day now

- Registry v3.2.0 due 2Q18 (funded)

  - ID Match via API

  - voPerson

  - Dashboards

- Registry v4.0.0 (tbd)

  - Framework Migration

MOO

SC

More Info

- Wiki

    - https://spaces.internet2.edu/display/COmanage

        – Technical Documentation

        – Data Model

    - https://spaces.internet2.edu/display/COmanage/Email+Lists

- Git

    - https://github.com/Internet2/comanage-registry

- TIER Packaging

    - https://spaces.internet2.edu/display/TPD

    - Docker