Internet2 COmanage Project

CoCoA Virtual Working Group

COmanage:

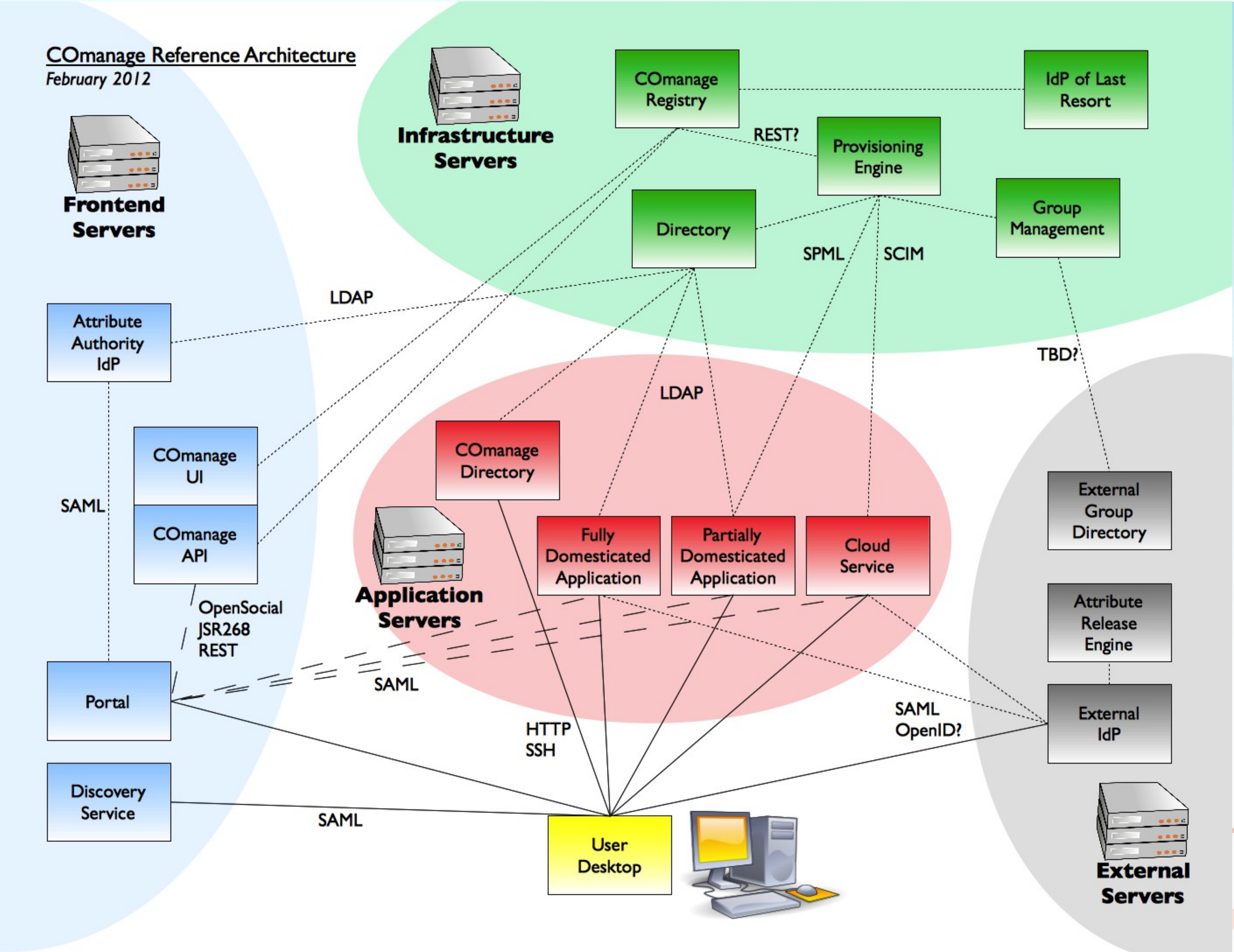
Person Attribute Management for Virtual Organizations and Collaborations

What is COmanage™ ?

- An identity management system system specifically designed for collaboration across campus boundaries
  - Federated and Social Identity
  - Identity Lifecycle Management
  - Onboarding and Offboarding Workflows
  - Attribute Management
  - Group Management
  - Provisioning
- Funded out of the NSF “Bedrock” SDCI grant

COmanage Reference Architecture

February 2012



Frontend Servers

Attribute Authority IdP

COmanage UI

COmanage API

Portal

Discovery Service

SAML

OpenSocial JSR268 REST

Infrastructure Servers

COmanage Registry

IdP of Last Resort

REST?

Provisioning Engine

Directory

Group Management

SPML

SCIM

LDAP

TBD?

Application Servers

COmanage Directory

Fully Domesticated Application

Partially Domesticated Application

Cloud Service

LDAP

SAML

HTTP SSH

SAML

User Desktop

SAML OpenID?

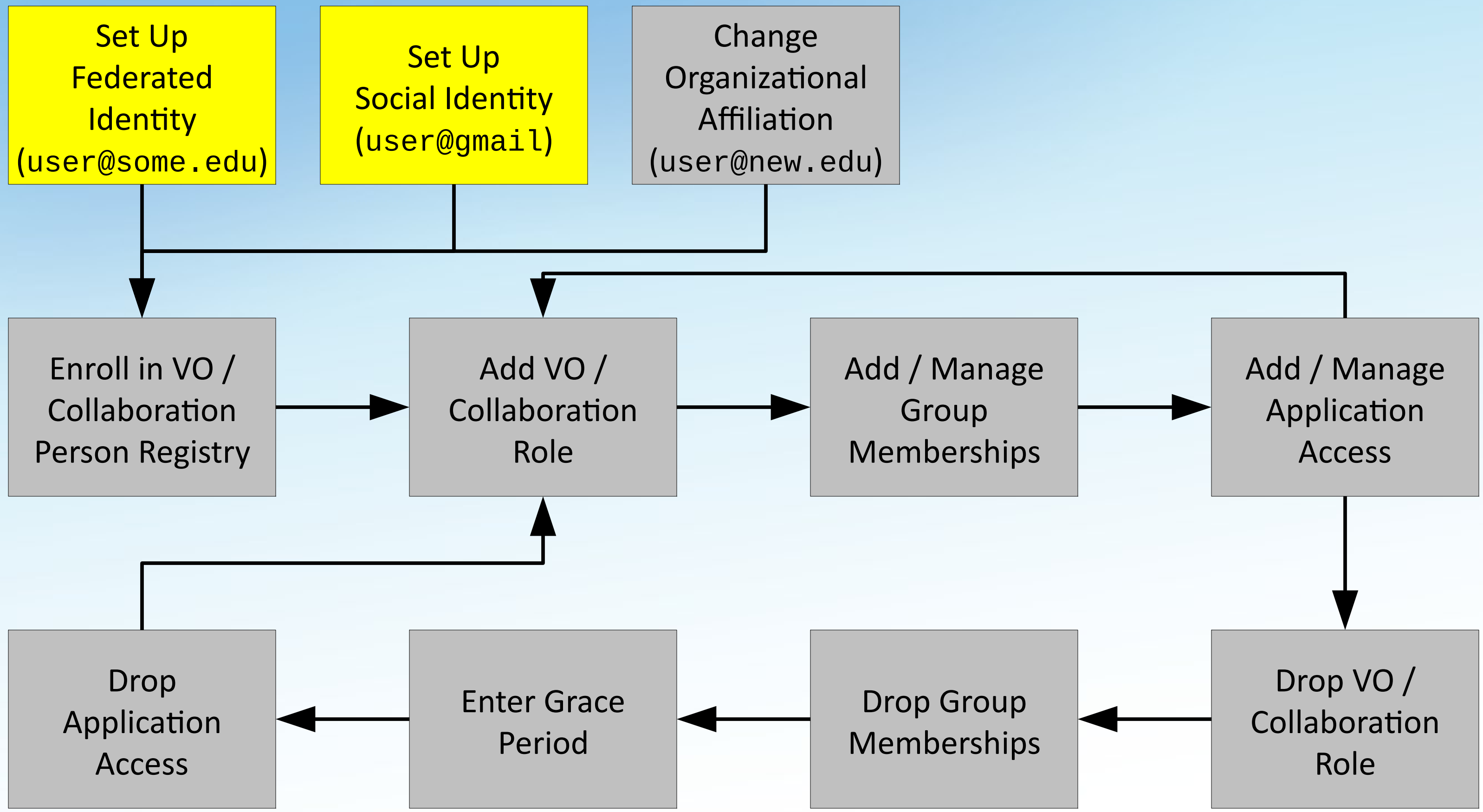
External Servers

External Group Directory

Attribute Release Engine

External IdP

Virtual / Collaborative Identity Lifecycle



Set Up Federated Identity (user@some.edu)

Set Up Social Identity (user@gmail)

Change Organizational Affiliation (user@new.edu)

Enroll in VO / Collaboration Person Registry

Add VO / Collaboration Role

Add / Manage Group Memberships

Add / Manage Application Access

Drop VO / Collaboration Role

Drop Group Memberships

Enter Grace Period

Drop Application Access

Organizational Identities

- Organizational Identities correlate with credential sources
- Organizational Identities *may* carry attributes
- Institutional / Federated Identity
  - Typically ePPN or ePTID via SAML
  - Attribute release from campus IdPs is a challenge
    - R&S bundle may help a bit
    - Approved SPs receive name / email / affiliation / userid without point-to-point negotiation

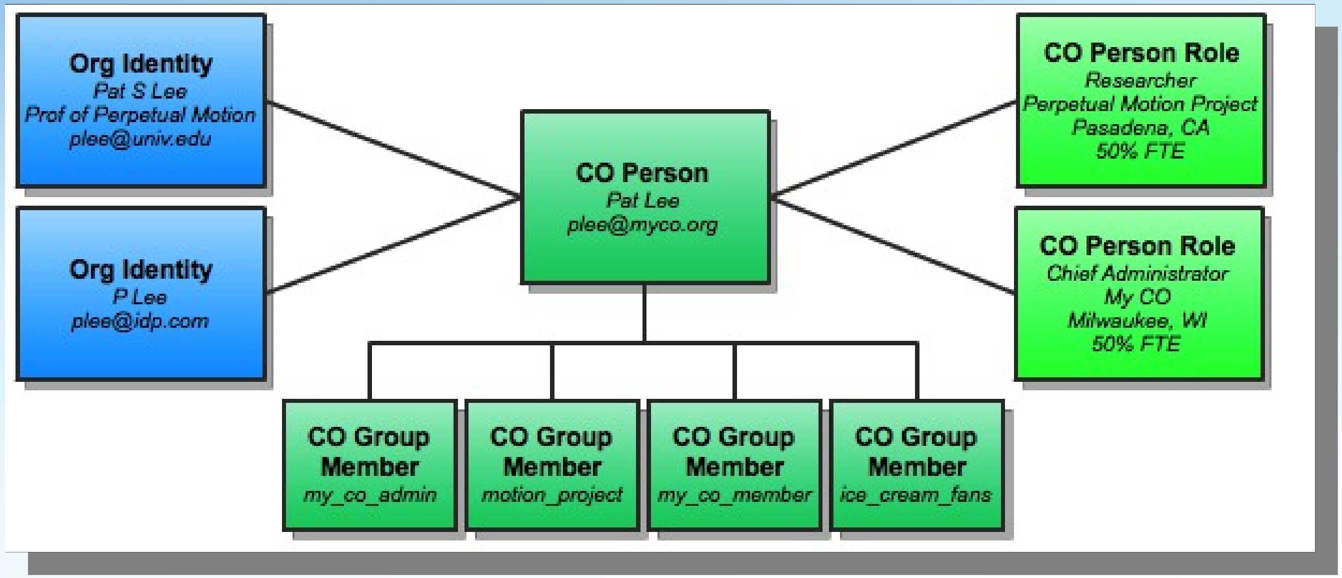
Organizational Identities

- Social Identity
  - Google / Facebook / Twitter / LinkedIn / etc
  - Various attributes typically easy to get, possibly with subject's approval
  - Gateways simplify integration (but that's the previous WG)
- VO Credentials
  - Larger VOs may need to issue their own credentials
  - Partly due to challenges in integrating federated identity
  - Partly due to security concerns
    - Perhaps one day InCommon Platinum™ will get you access to the interferometer

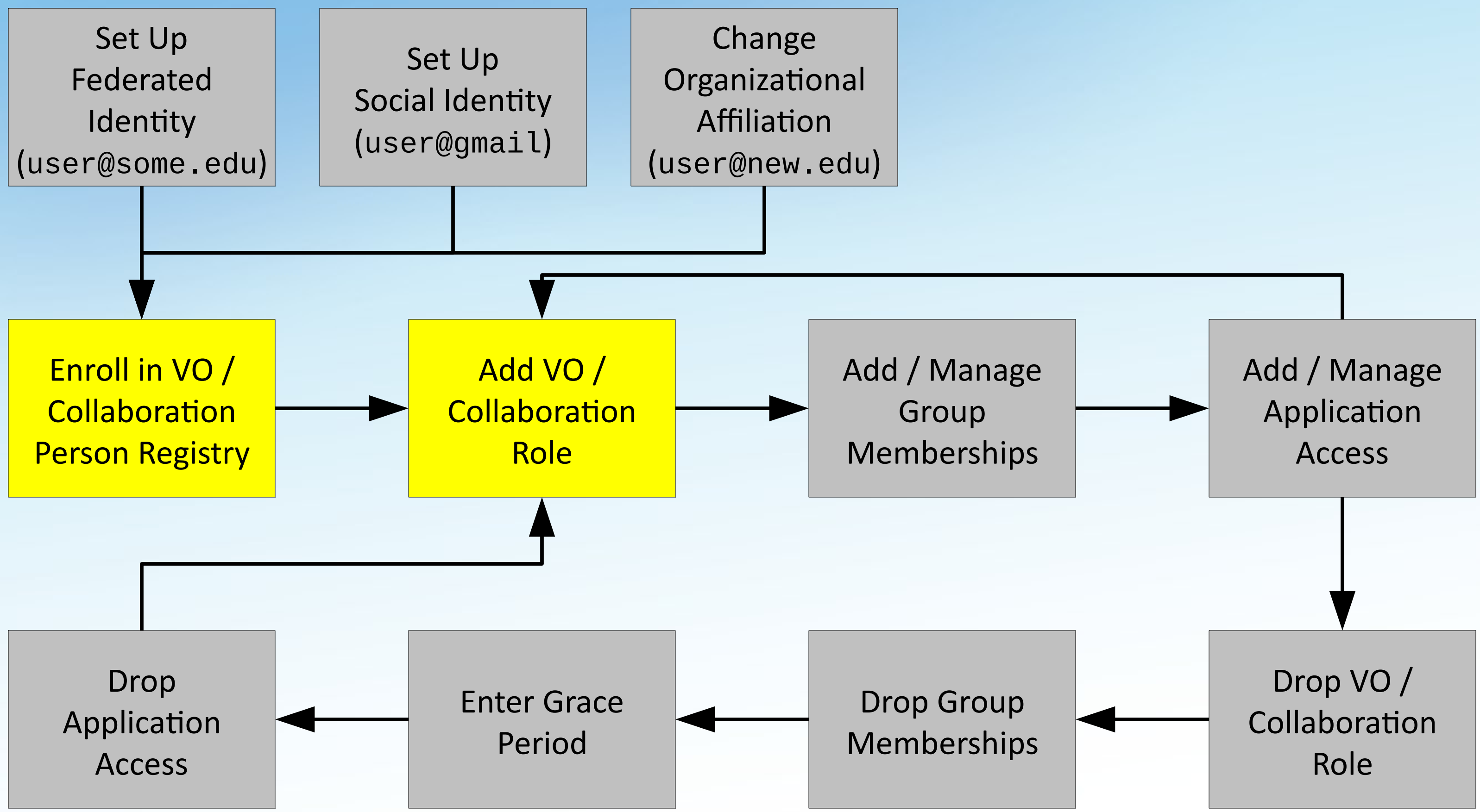
VO / Collaboration Identities

- Associated with one or more Organizational Identities
- VO / Collaboration Attributes
  - Name (eg: Author Name)
  - Email Address (`user@myvo.org`)
  - Directory Attributes
  - Role-Specific Attributes
    - Title
    - Start / End Dates
    - Extended Attributes
  - Group Memberships

VO / Collaboration Identities



Virtual / Collaborative Identity Lifecycle



Set Up Federated Identity (user@some.edu)

Set Up Social Identity (user@gmail)

Change Organizational Affiliation (user@new.edu)

Enroll in VO / Collaboration Person Registry

Add VO / Collaboration Role

Add / Manage Group Memberships

Add / Manage Application Access

Drop VO / Collaboration Role

Drop Group Memberships

Enter Grace Period

Drop Application Access

Enrollment Terminology

- A **CO Administrator** is in charge of the VO / Collaboration
- A **COU Administrator** is in charge of a sub-population of the CO
- The CO Admin defines one or more **Enrollment Flows** to control how new members **("Enrollees")** are added to the Collaboration
- A **Petitioner** executes an Enrollment Flow by creating a **Petition** in order to add an Enrollee to the Collaboration
- An **Approver** reviews the Petition

Common Enrollment Patterns

- **Conscription**: Petitioner adds enrollee, possibly requiring approval, but without enrollee confirmation
- **Invitation**: Petitioner invites enrollee, possibly requiring approval; Enrollee confirms before becoming active
- **Self-Signup**: Enrollee is also petitioner; No approval required
- **Application**: Enrollee is also petitioner; Approval required
- **Account Linking**: Enrollee is also petitioner; Enrollee already exists in Collaboration and wishes to add a new organizational identity (federated or social)

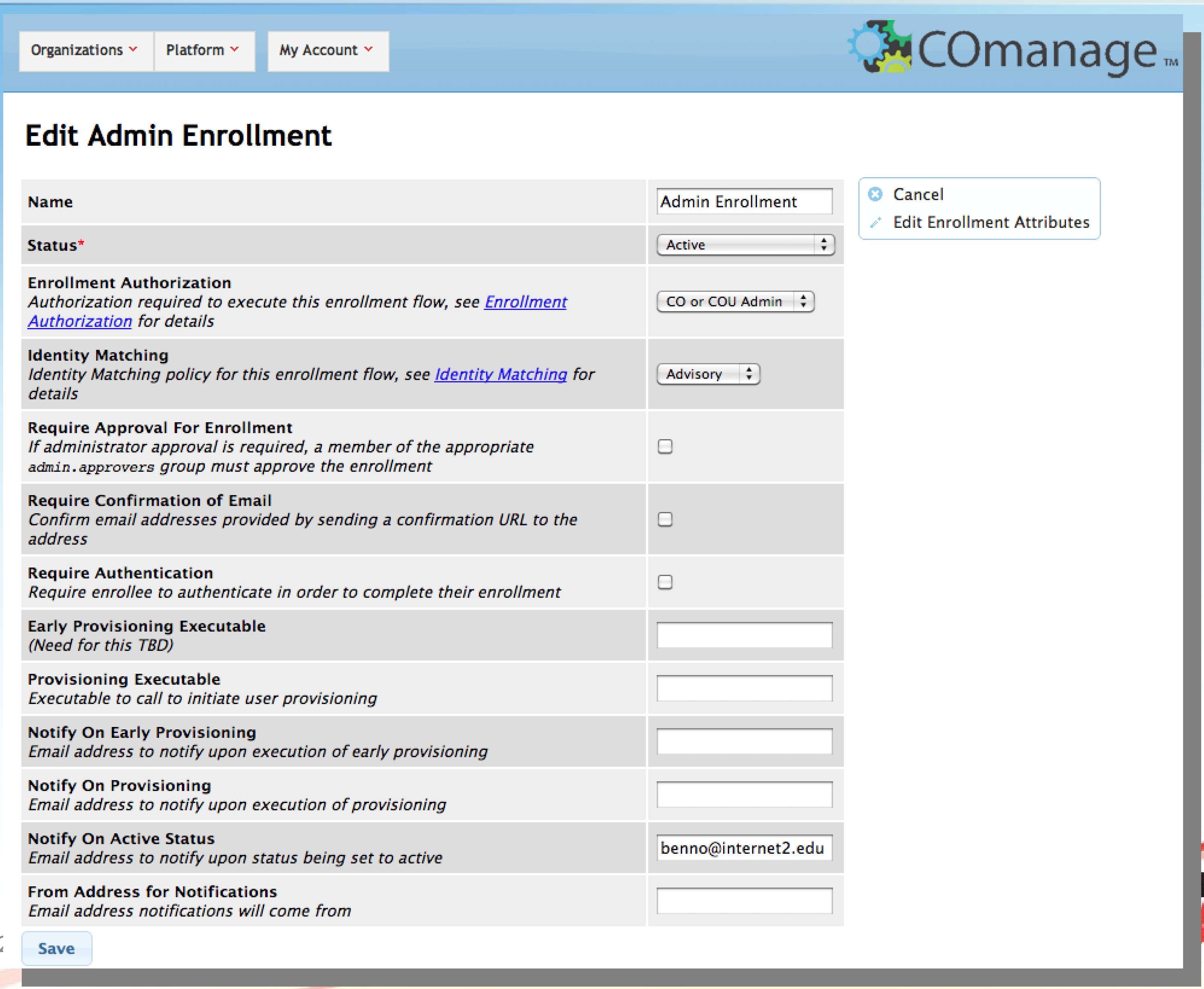
Enrollment Actors

	Large VO	Community Collaboration	Tenure Committee
Petitioner	Hiring Manager / Administrator	Any Existing Member	Department Administrator
Enrollee	•New Researcher •Scientific Reviewer •Undergraduates (Summer Program)	•Students in K-12 •Faculty in Univ Depts •Community Members	Committee Member
Approver	VO Director	Designated Community Leaders	Department Chair

Enrollment (Simplified)

- Petitioner completes form of required and optional attributes, as configured for the enrollment flow
- Registry performs identity match to determine if enrollee is already known to the Collaboration
- Enrollee authenticates to demonstrate control over organizational identity credentials
- Approver reviews Petition
- Enrollee becomes active
- Attributes become available to downstream applications

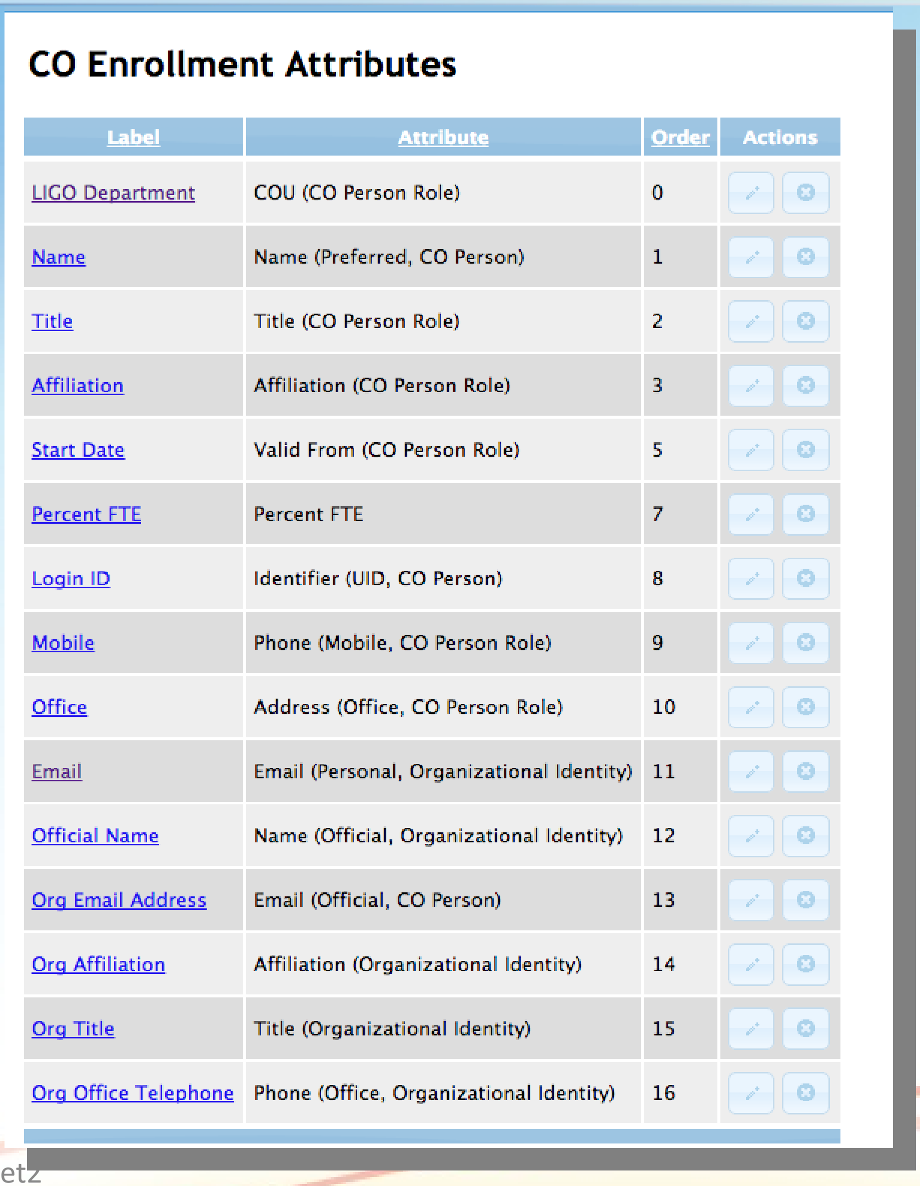
Enrollment Flow Configuration



Edit Admin Enrollment

Name	Admin Enrollment
Status*	Active
Enrollment Authorization *Authorization required to execute this enrollment flow, see Enrollment Authorization for details*	CO or COU Admin
Identity Matching *Identity Matching policy for this enrollment flow, see Identity Matching for details*	Advisory
Require Approval For Enrollment *If administrator approval is required, a member of the appropriate `admin.approvers` group must approve the enrollment*	□
Require Confirmation of Email *Confirm email addresses provided by sending a confirmation URL to the address*	□
Require Authentication *Require enrollee to authenticate in order to complete their enrollment*	□
Early Provisioning Executable *(Need for this TBD)*	
Provisioning Executable *Executable to call to initiate user provisioning*	
Notify On Early Provisioning *Email address to notify upon execution of early provisioning*	
Notify On Provisioning *Email address to notify upon execution of provisioning*	
Notify On Active Status *Email address to notify upon status being set to active*	benno@internet2.edu
From Address for Notifications *Email address notifications will come from*	

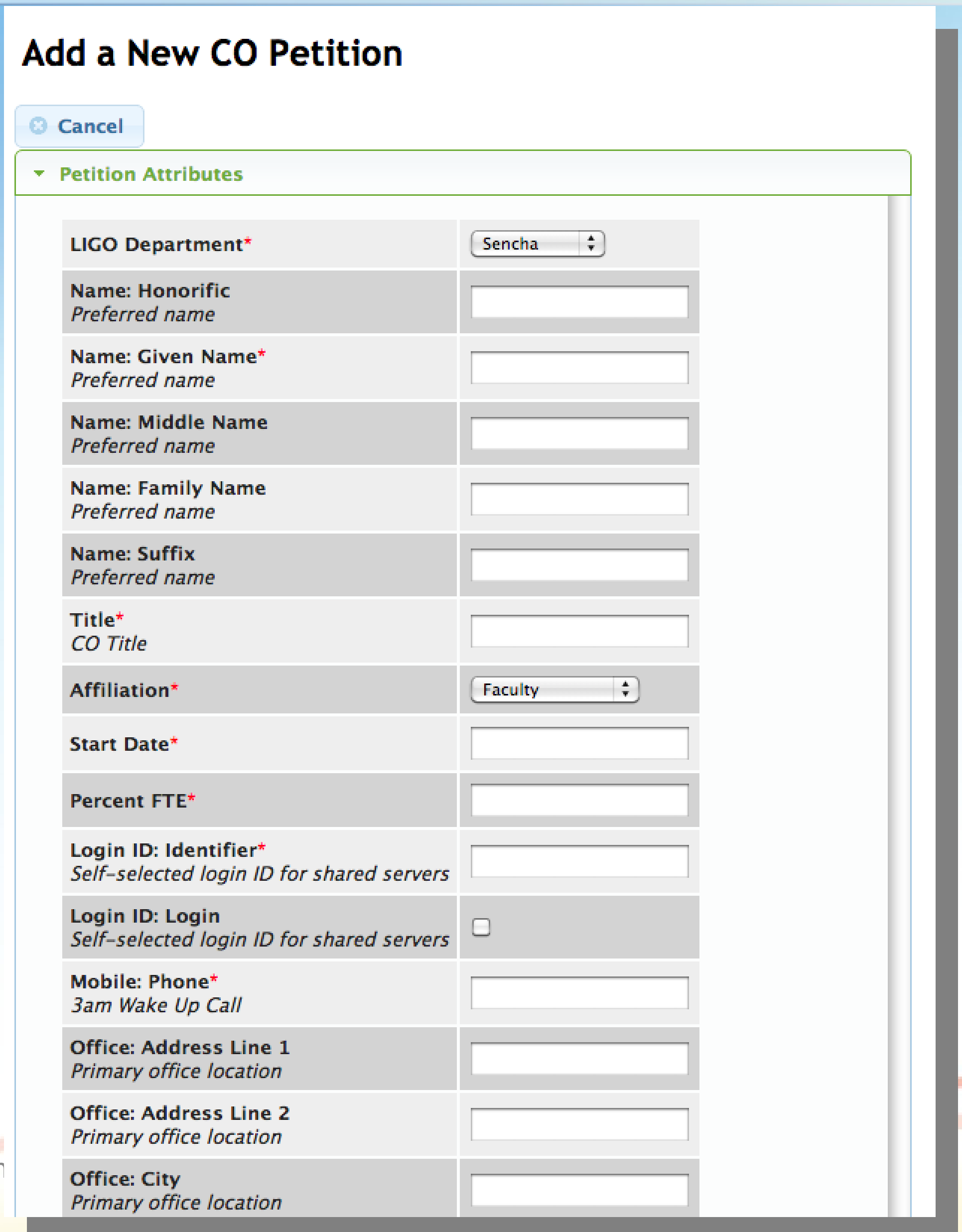
Enrollment Flow Configuration



CO Enrollment Attributes

Label	Attribute	Order	Actions
LIGO Department	COU (CO Person Role)	0	✎ ⊗
Name	Name (Preferred, CO Person)	1	✎ ⊗
Title	Title (CO Person Role)	2	✎ ⊗
Affiliation	Affiliation (CO Person Role)	3	✎ ⊗
Start Date	Valid From (CO Person Role)	5	✎ ⊗
Percent FTE	Percent FTE	7	✎ ⊗
Login ID	Identifier (UID, CO Person)	8	✎ ⊗
Mobile	Phone (Mobile, CO Person Role)	9	✎ ⊗
Office	Address (Office, CO Person Role)	10	✎ ⊗
Email	Email (Personal, Organizational Identity)	11	✎ ⊗
Official Name	Name (Official, Organizational Identity)	12	✎ ⊗
Org Email Address	Email (Official, CO Person)	13	✎ ⊗
Org Affiliation	Affiliation (Organizational Identity)	14	✎ ⊗
Org Title	Title (Organizational Identity)	15	✎ ⊗
Org Office Telephone	Phone (Office, Organizational Identity)	16	✎ ⊗

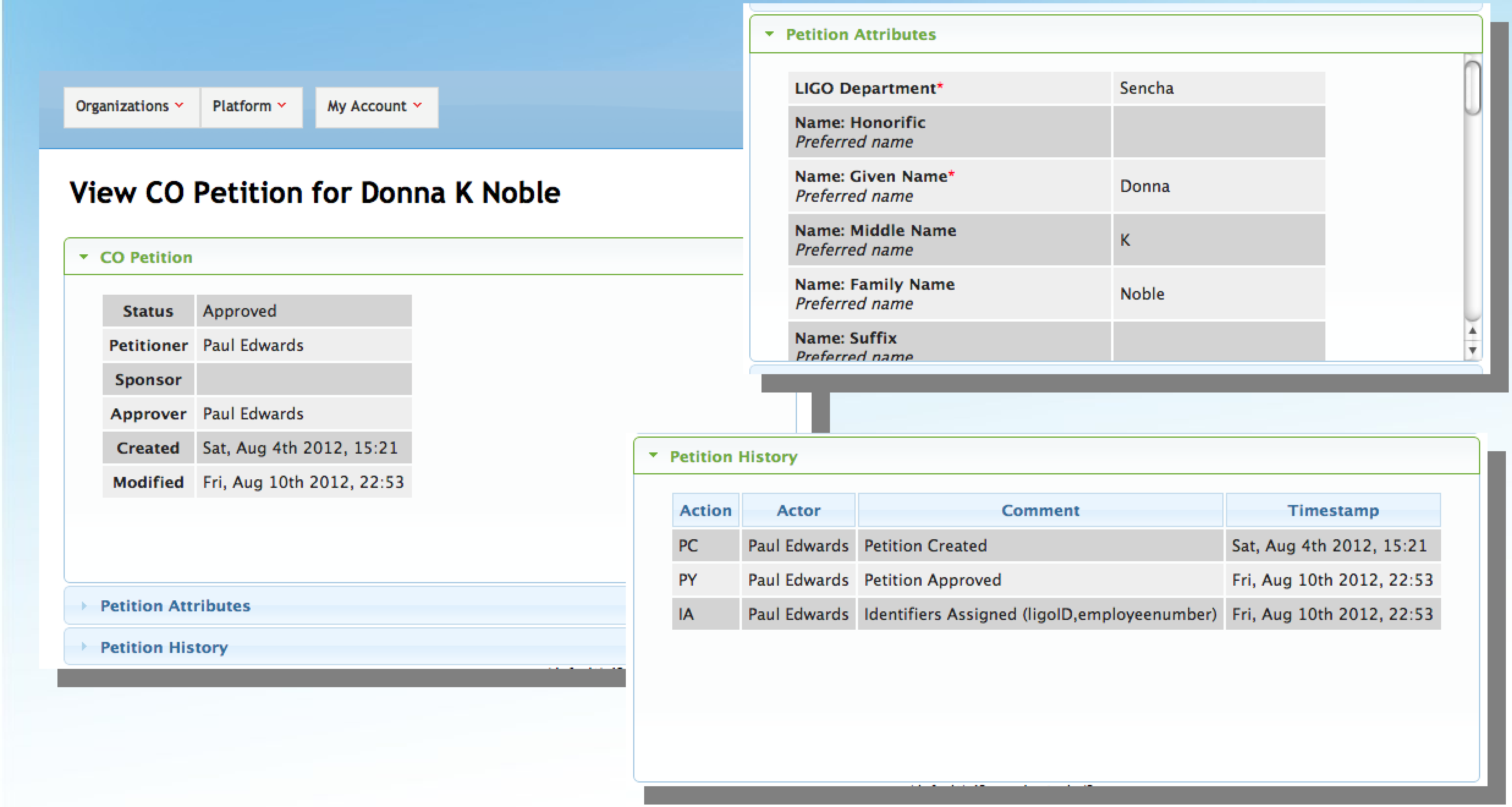
Creating a Petition



Add a New CO Petition

LIGO Department*	Sencha
Name: Honorific *Preferred name*	
Name: Given Name* *Preferred name*	
Name: Middle Name *Preferred name*	
Name: Family Name *Preferred name*	
Name: Suffix *Preferred name*	
Title* *CO Title*	
Affiliation*	Faculty
Start Date*	
Percent FTE*	
Login ID: Identifier* *Self-selected login ID for shared servers*	
Login ID: Login *Self-selected login ID for shared servers*	☐
Mobile: Phone* *3am Wake Up Call*	
Office: Address Line 1 *Primary office location*	
Office: Address Line 2 *Primary office location*	
Office: City *Primary office location*	

Reviewing a Petition



View CO Petition for Donna K Noble

CO Petition

Status	Approved
Petitioner	Paul Edwards
Sponsor	
Approver	Paul Edwards
Created	Sat, Aug 4th 2012, 15:21
Modified	Fri, Aug 10th 2012, 22:53

Petition Attributes

Petition History

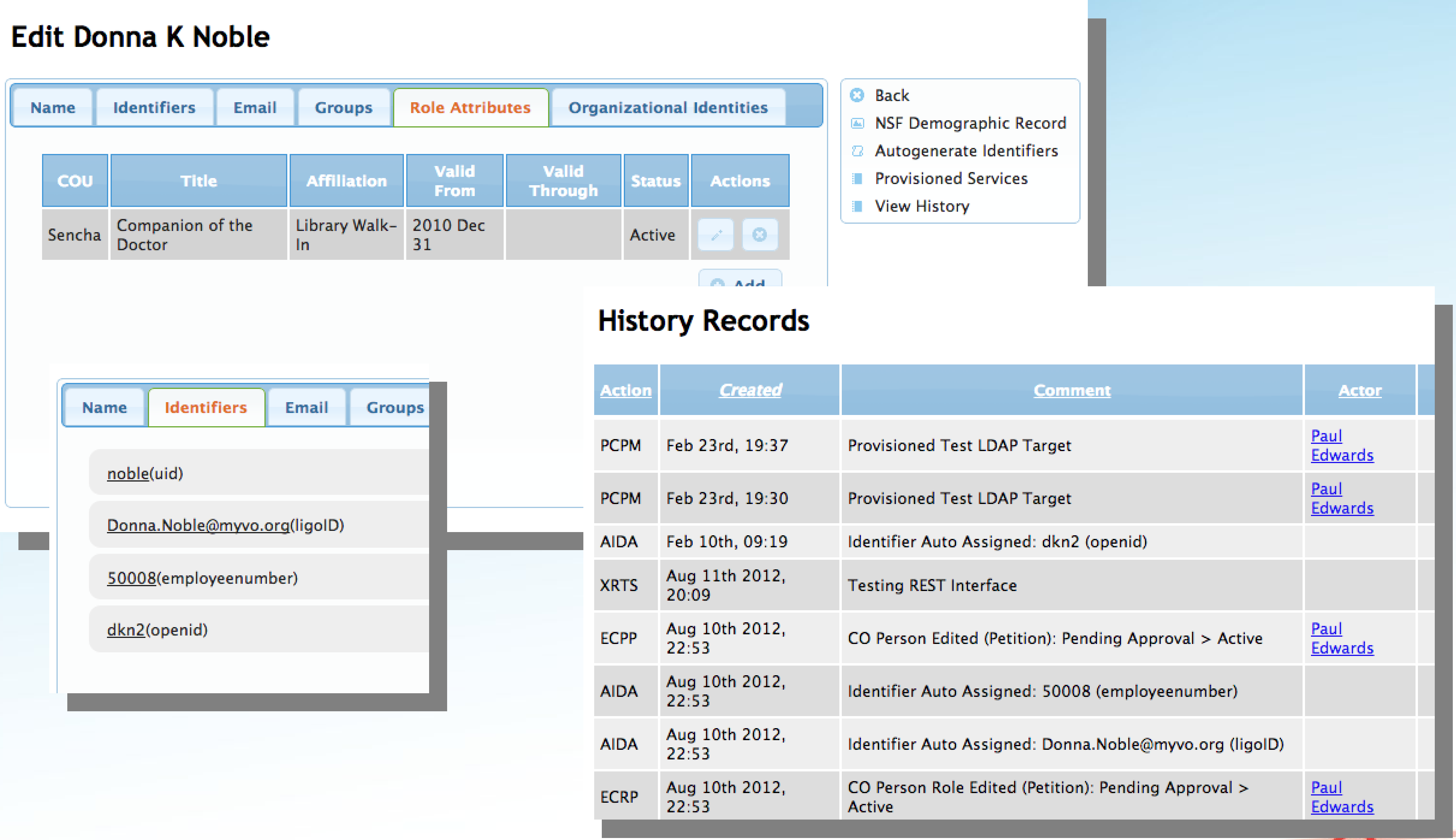
Petition Attributes

LIGO Department*	Sencha
Name: Honorific *Preferred name*	
Name: Given Name* *Preferred name*	Donna
Name: Middle Name *Preferred name*	K
Name: Family Name *Preferred name*	Noble
Name: Suffix *Preferred name*	

Petition History

Action	Actor	Comment	Timestamp
PC	Paul Edwards	Petition Created	Sat, Aug 4th 2012, 15:21
PY	Paul Edwards	Petition Approved	Fri, Aug 10th 2012, 22:53
IA	Paul Edwards	Identifiers Assigned (ligoID,employeenumber)	Fri, Aug 10th 2012, 22:53

Creating a Petition



Edit Donna K Noble

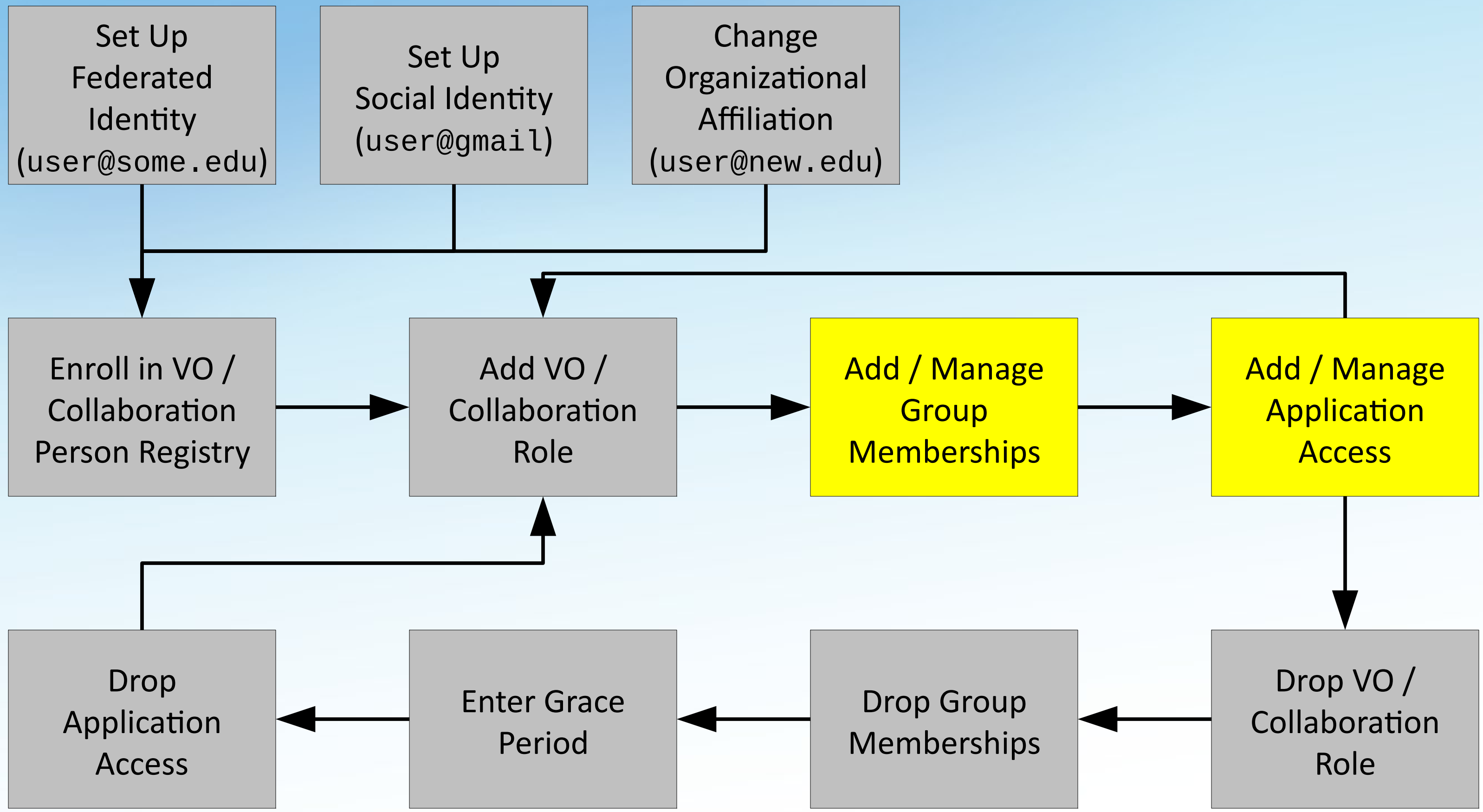
COU	Title	Affiliation	Valid From	Valid Through	Status	Actions
Sencha	Companion of the Doctor	Library Walk-In	2010 Dec 31		Active	

- noble(uid)
- Donna.Noble@myvo.org(ligoID)
- 50008(employeenumber)
- dkn2(openid)

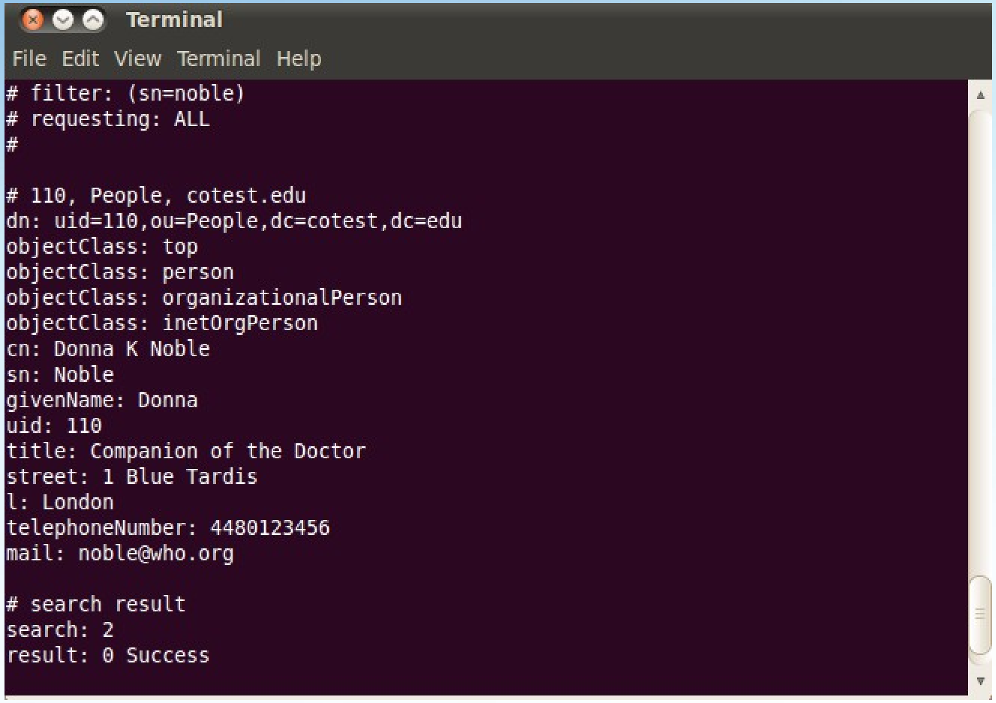
History Records

Action	Created	Comment	Actor
PCPM	Feb 23rd, 19:37	Provisioned Test LDAP Target	Paul Edwards
PCPM	Feb 23rd, 19:30	Provisioned Test LDAP Target	Paul Edwards
AIDA	Feb 10th, 09:19	Identifier Auto Assigned: dkn2 (openid)	
XRTS	Aug 11th 2012, 20:09	Testing REST Interface	
ECPP	Aug 10th 2012, 22:53	CO Person Edited (Petition): Pending Approval > Active	Paul Edwards
AIDA	Aug 10th 2012, 22:53	Identifier Auto Assigned: 50008 (employeenumber)	
AIDA	Aug 10th 2012, 22:53	Identifier Auto Assigned: Donna.Noble@myvo.org (ligoID)	
ECRP	Aug 10th 2012, 22:53	CO Person Role Edited (Petition): Pending Approval > Active	Paul Edwards

Virtual / Collaborative Identity Lifecycle

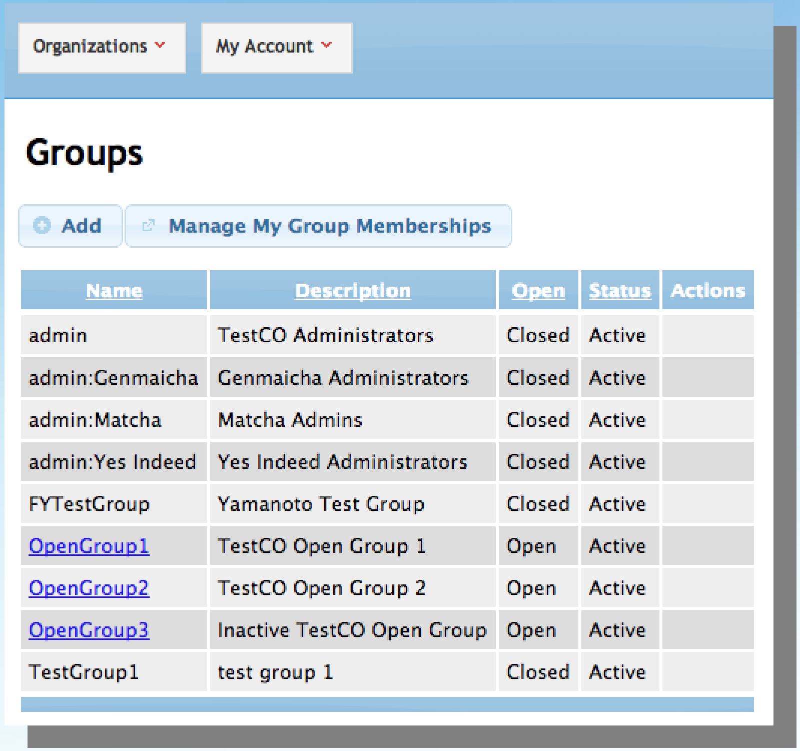

Set Up Federated Identity (user@some.edu)
Set Up Social Identity (user@gmail)
Change Organizational Affiliation (user@new.edu)
Enroll in VO / Collaboration Person Registry
Add VO / Collaboration Role
Add / Manage Group Memberships
Add / Manage Application Access
Drop Application Access
Enter Grace Period
Drop Group Memberships
Drop VO / Collaboration Role

Provisioning LDAP



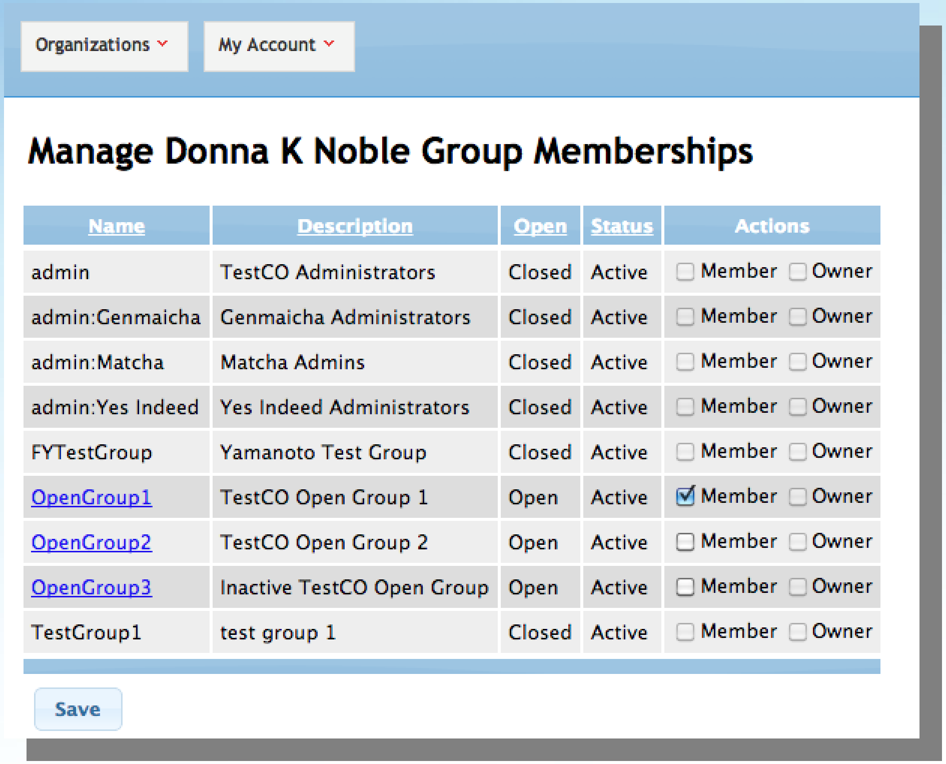
```
# filter: (sn=noble)
# requesting: ALL
#

# 110, People, cotest.edu
dn: uid=110,ou=People,dc=cotest,dc=edu
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: Donna K Noble
sn: Noble
givenName: Donna
uid: 110
title: Companion of the Doctor
street: 1 Blue Tardis
l: London
telephoneNumber: 4480123456
mail: noble@who.org

# search result
search: 2
result: 0 Success
```

Group Management



Groups

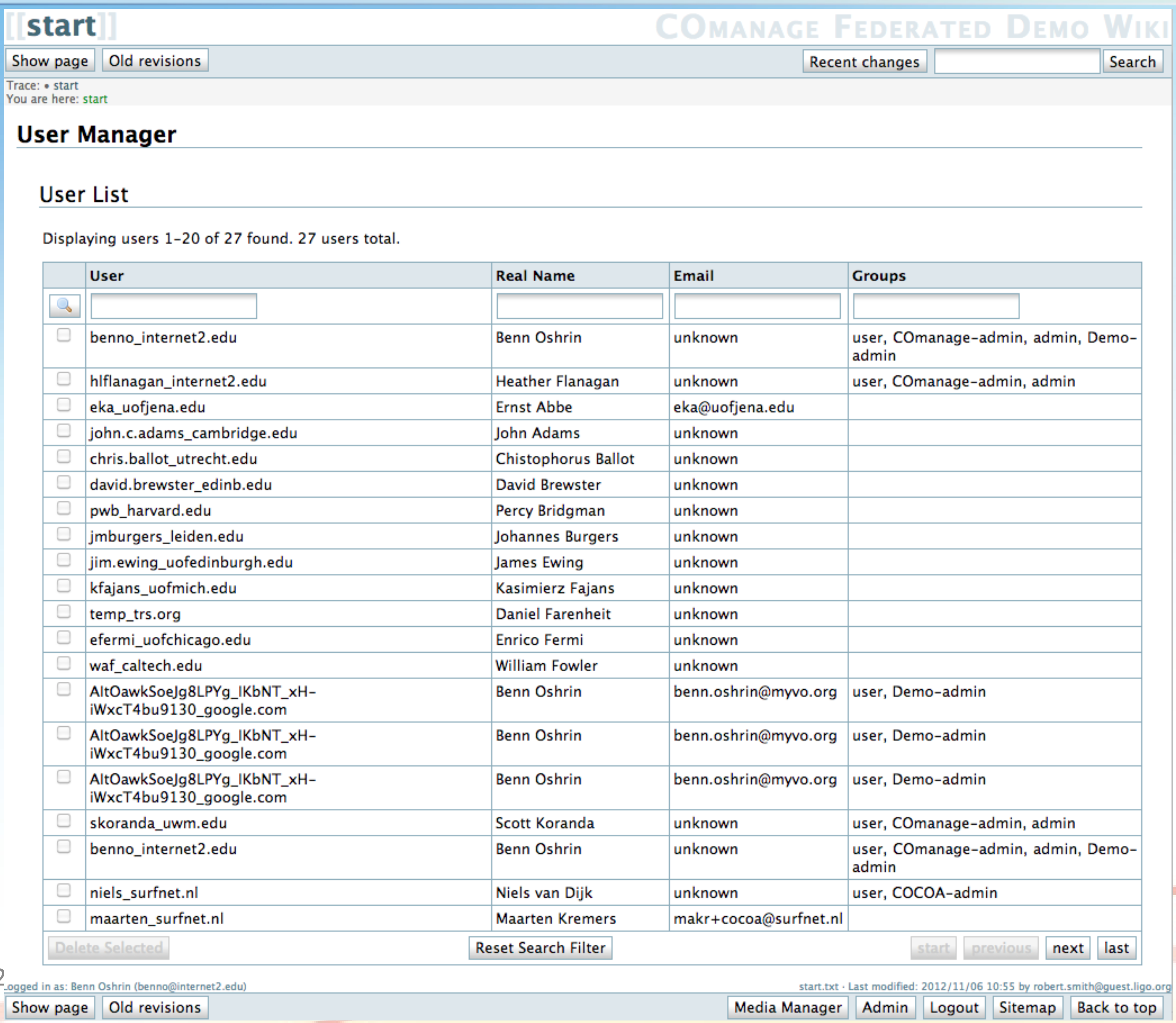
Name	Description	Open	Status	Actions
admin	TestCO Administrators	Closed	Active	
admin:Genmaicha	Genmaicha Administrators	Closed	Active	
admin:Matcha	Matcha Admins	Closed	Active	
admin:Yes Indeed	Yes Indeed Administrators	Closed	Active	
FYTestGroup	Yamanoto Test Group	Closed	Active	
OpenGroup1	TestCO Open Group 1	Open	Active	
OpenGroup2	TestCO Open Group 2	Open	Active	
OpenGroup3	Inactive TestCO Open Group	Open	Active	
TestGroup1	test group 1	Closed	Active	



Manage Donna K Noble Group Memberships

Name	Description	Open	Status	Actions
admin	TestCO Administrators	Closed	Active	□ Member □ Owner
admin:Genmaicha	Genmaicha Administrators	Closed	Active	□ Member □ Owner
admin:Matcha	Matcha Admins	Closed	Active	□ Member □ Owner
admin:Yes Indeed	Yes Indeed Administrators	Closed	Active	□ Member □ Owner
FYTestGroup	Yamanoto Test Group	Closed	Active	□ Member □ Owner
OpenGroup1	TestCO Open Group 1	Open	Active	☑ Member □ Owner
OpenGroup2	TestCO Open Group 2	Open	Active	□ Member □ Owner
OpenGroup3	Inactive TestCO Open Group	Open	Active	□ Member □ Owner
TestGroup1	test group 1	Closed	Active	□ Member □ Owner

Sample Wiki



Trace: • start
You are here: start

User Manager

User List

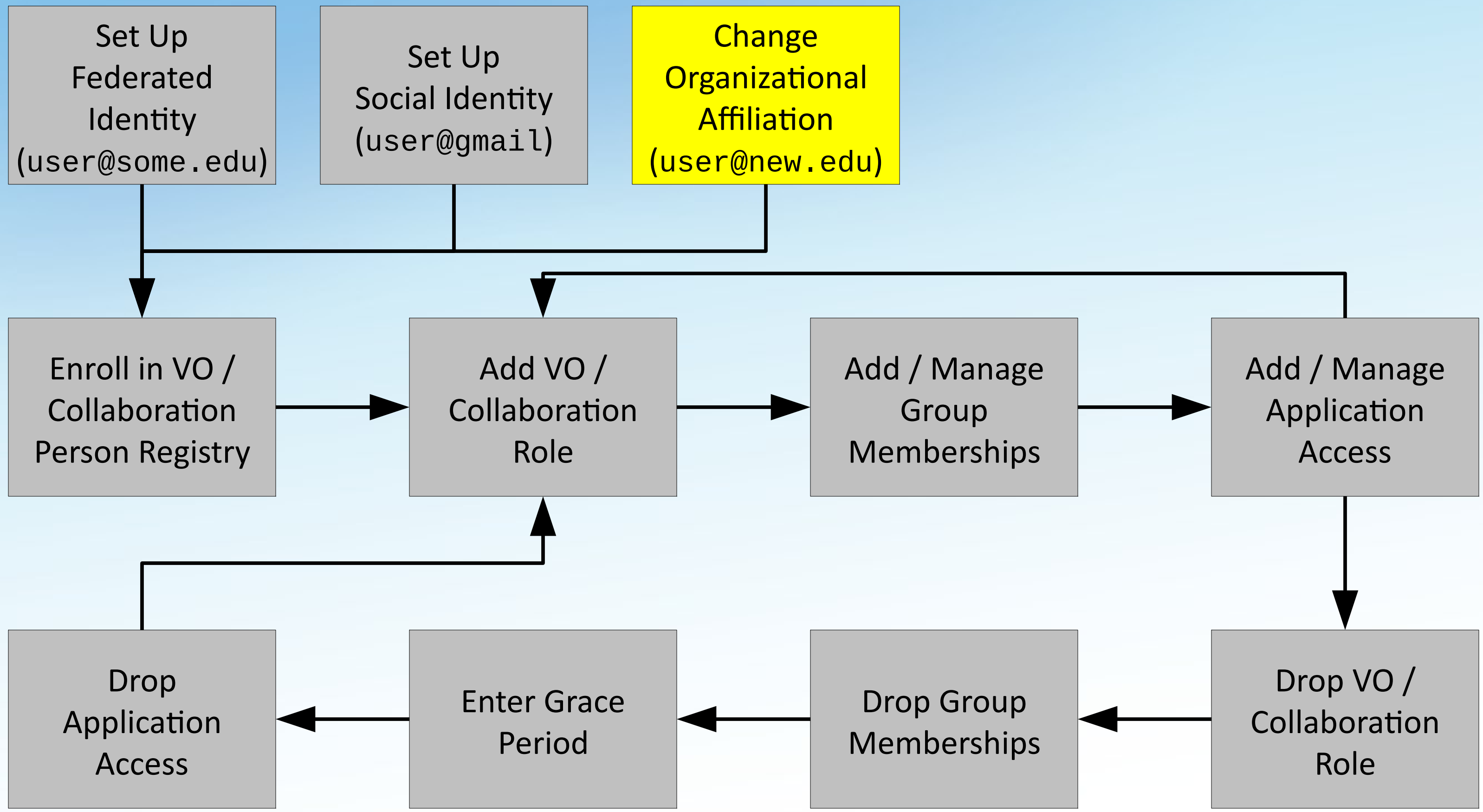
Displaying users 1-20 of 27 found. 27 users total.

	User	Real Name	Email	Groups
□	benno_internet2.edu	Benn Oshrin	unknown	user, COmanage-admin, admin, Demo-admin
□	hlflanagan_internet2.edu	Heather Flanagan	unknown	user, COmanage-admin, admin
□	eka_uofjena.edu	Ernst Abbe	eka@uofjena.edu	
□	john.c.adams_cambridge.edu	John Adams	unknown	
□	chris.ballot_utrecht.edu	Chistophorus Ballot	unknown	
□	david.brewster_edinb.edu	David Brewster	unknown	
□	pwb_harvard.edu	Percy Bridgman	unknown	
□	jmburgers_leiden.edu	Johannes Burgers	unknown	
□	jim.ewing_uofedinburgh.edu	James Ewing	unknown	
□	kfajans_uofmich.edu	Kasimierz Fajans	unknown	
□	temp_trs.org	Daniel Farenheit	unknown	
□	efermi_uofchicago.edu	Enrico Fermi	unknown	
□	waf_caltech.edu	William Fowler	unknown	
□	AltOawkSoeJg8LPYg_IKbNT_xH-iWxcT4bu9130_google.com	Benn Oshrin	benn.oshrin@myvo.org	user, Demo-admin
□	AltOawkSoeJg8LPYg_IKbNT_xH-iWxcT4bu9130_google.com	Benn Oshrin	benn.oshrin@myvo.org	user, Demo-admin
□	AltOawkSoeJg8LPYg_IKbNT_xH-iWxcT4bu9130_google.com	Benn Oshrin	benn.oshrin@myvo.org	user, Demo-admin
□	skoranda_uwm.edu	Scott Koranda	unknown	user, COmanage-admin, admin
□	benno_internet2.edu	Benn Oshrin	unknown	user, COmanage-admin, admin, Demo-admin
□	niels_surfnet.nl	Niels van Dijk	unknown	user, COCOA-admin
□	maarten_surfnet.nl	Maarten Kremers	makr+cocoa@surfnet.nl	

ogged in as: Benn Oshrin (benno@internet2.edu)

start.txt · Last modified: 2012/11/06 10:55 by robert.smith@guest.ligo.org

Virtual / Collaborative Identity Lifecycle



Set Up Federated Identity (user@some.edu)

Set Up Social Identity (user@gmail)

Change Organizational Affiliation (user@new.edu)

Enroll in VO / Collaboration Person Registry

Add VO / Collaboration Role

Add / Manage Group Memberships

Add / Manage Application Access

Drop VO / Collaboration Role

Drop Group Memberships

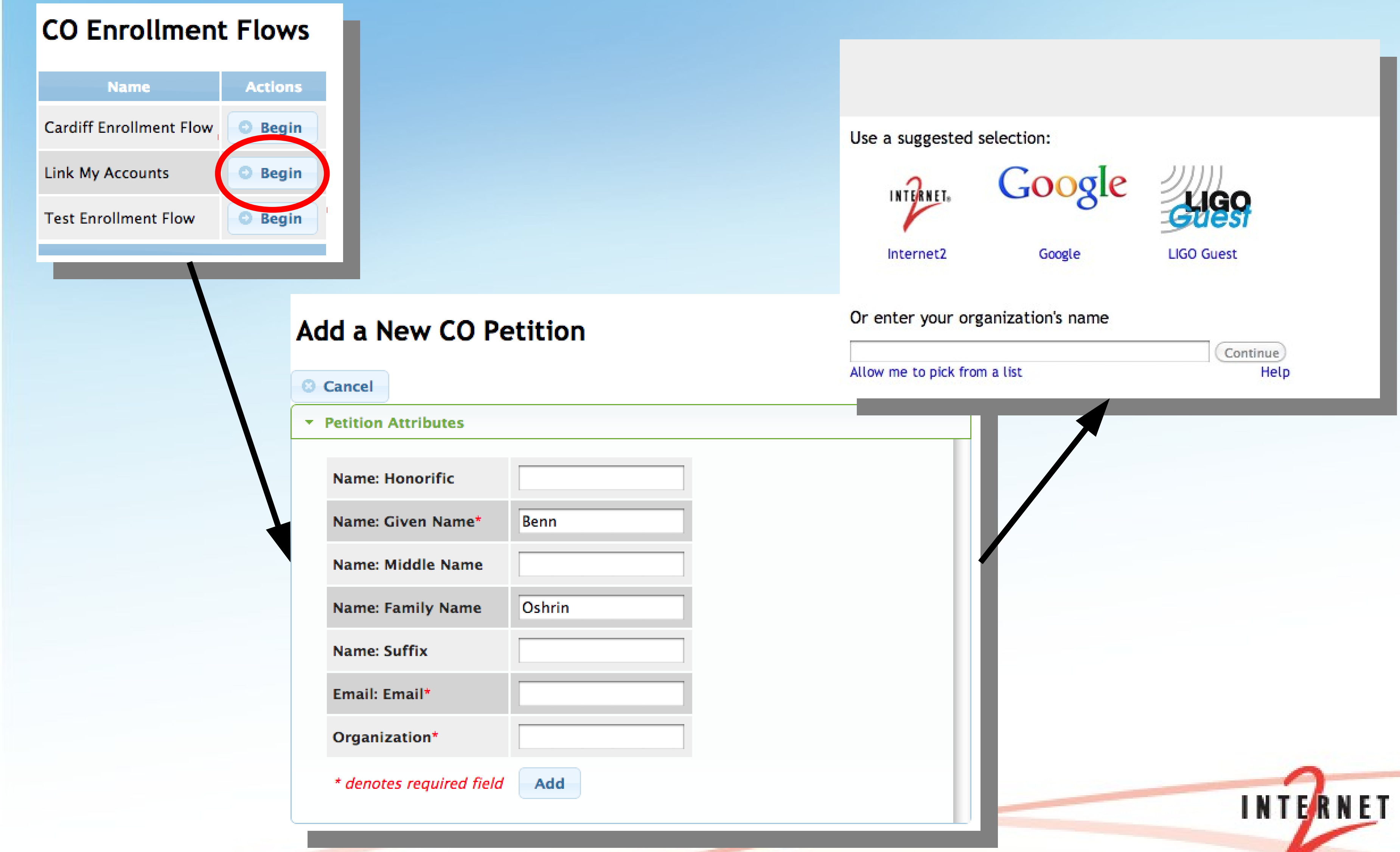
Enter Grace Period

Drop Application Access

Organizational Migration

- Members of a Collaboration often change institutional affiliation during their work with the Collaboration
- Account Linking enrollment can allow a person to transition on their own
- Collaboration attributes remain attached to the CO Person record, not to the Organizational Identity
- Requires care in integrating applications (which identifier to use?)

Account Linking



CO Enrollment Flows

Name	Actions
Cardiff Enrollment Flow	Begin
Link My Accounts	Begin
Test Enrollment Flow	Begin

Add a New CO Petition

Cancel

▾ Petition Attributes

Name: Honorific	
Name: Given Name*	Benn
Name: Middle Name	
Name: Family Name	Oshrin
Name: Suffix	
Email: Email*	
Organization*	

** denotes required field*

Add

Use a suggested selection:

Internet2 Google LIGO Guest

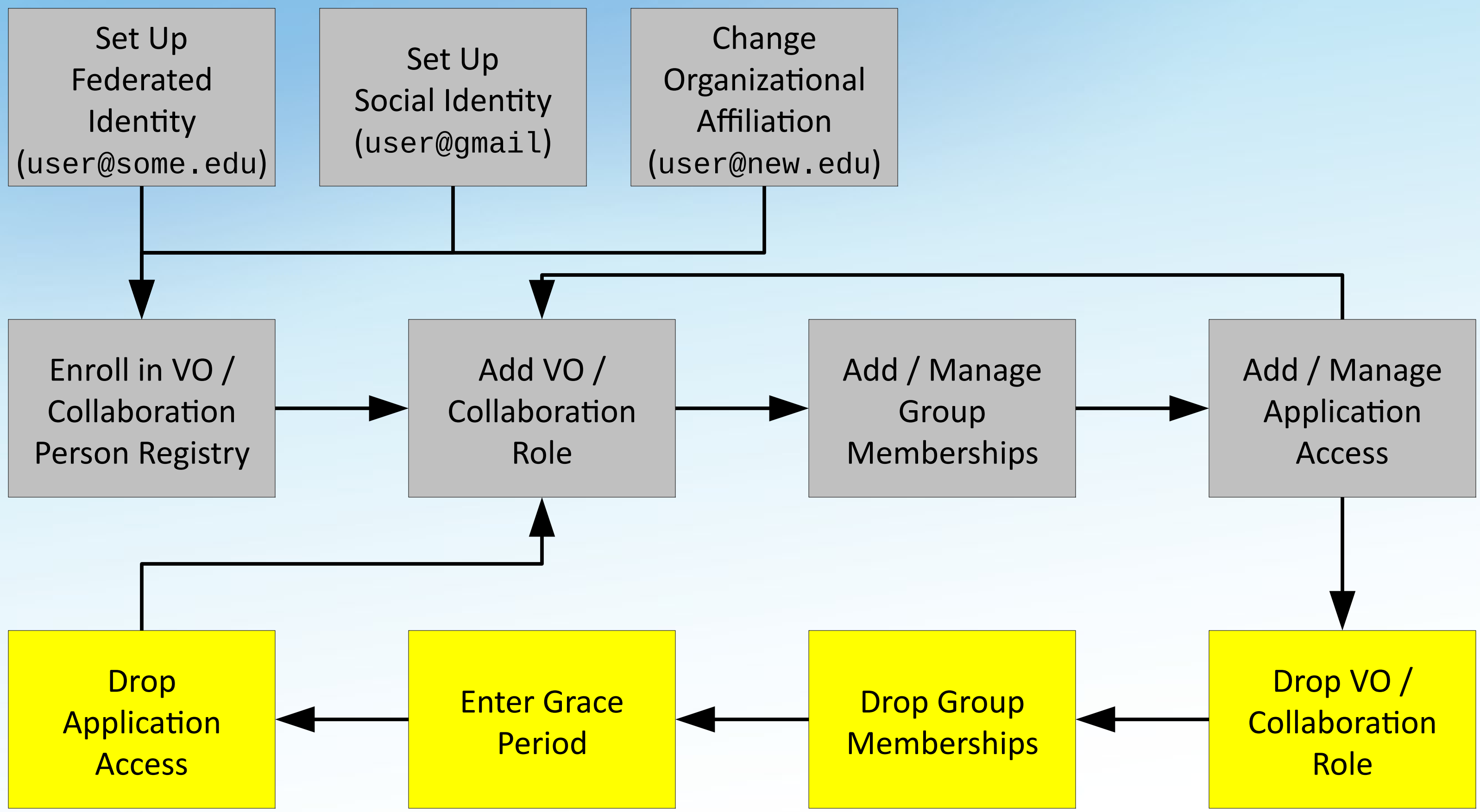
Or enter your organization's name

Continue

Allow me to pick from a list

Help

Virtual / Collaborative Identity Lifecycle



Set Up Federated Identity (user@some.edu)

Set Up Social Identity (user@gmail)

Change Organizational Affiliation (user@new.edu)

Enroll in VO / Collaboration Person Registry

Add VO / Collaboration Role

Add / Manage Group Memberships

Add / Manage Application Access

Drop VO / Collaboration Role

Drop Group Memberships

Enter Grace Period

Drop Application Access

Offboarding

- Offboarding may happen for a variety of reasons
- Approval may be required
- The usual “clean up” issues apply
  - Grace Periods may be initiated for some services
  - What happens to data? (Archive vs delete)

Common Offboarding Patterns

- **Expiration**: Fixed duration of participation (possibly determined at Enrollment) has been completed
- **Termination**: Separation initiated by Collaboration
- **Resignation**: Separation initiated by Participant
- **Desertion**: Participant stops participating, does not give notice
- **Retirement**: More applicable to larger VOs
- **Leave of Absence**: Triggers deprovisioning, with re-provisioning when return date reached

OpenConext:

Group-Based, Federated Collaboration Tools

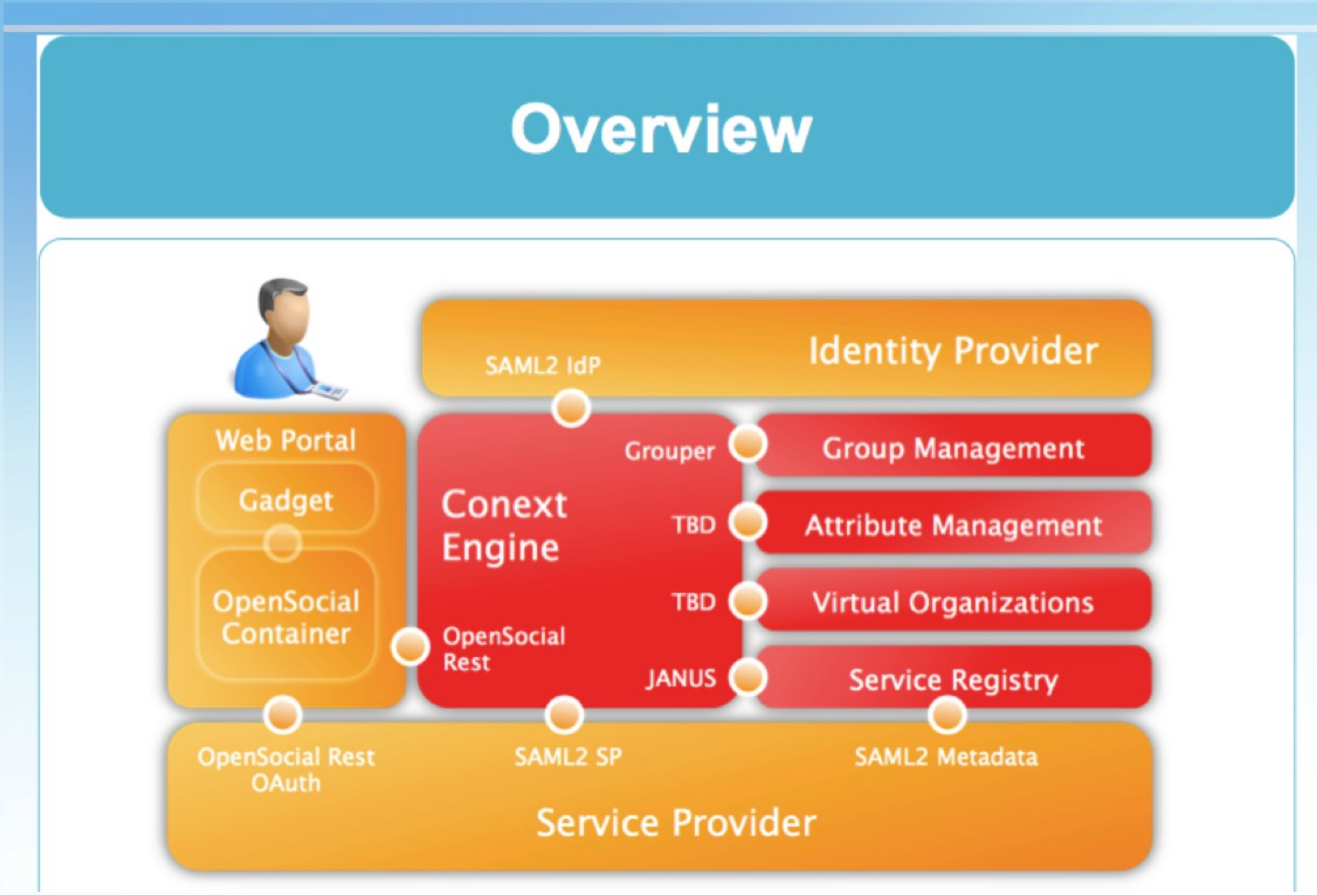
OpenConext

- OpenConext is an OpenSource collaboration platform developed by SURFnet (the Dutch NREN)
- Designed to make collaboration easy for users, who should be able to
  - Use their own favourite tools as much as possible
  - Re-use their credentials (username/password) for every tool they use
  - Create their own collaboration groups and re-use those for every tool as well

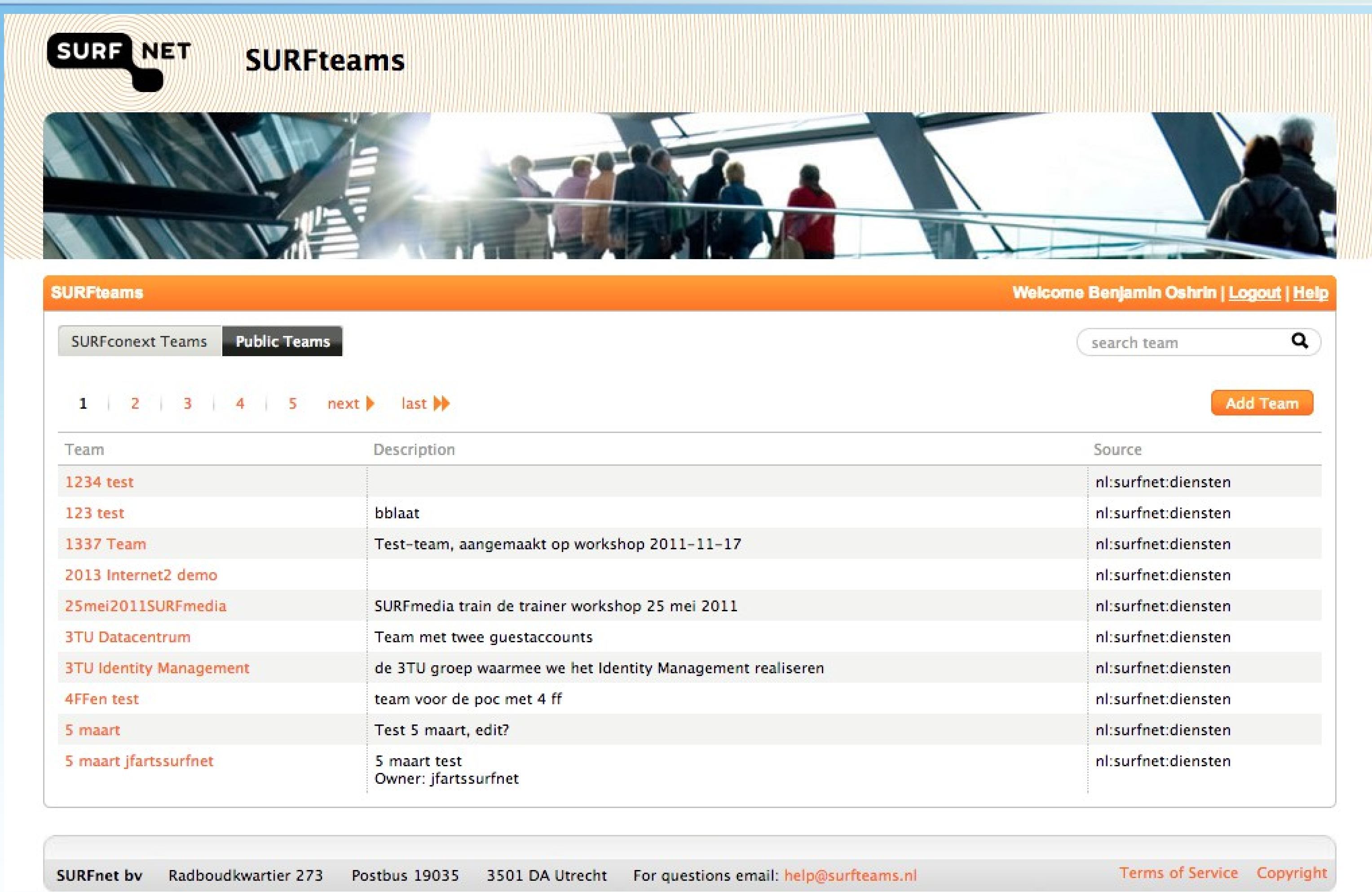
OpenConext

- OpenSocial-centric design built on OpenSource tools/products including
  - Corto, Janus, Apache Shindig, Apache Rave
  - Grouper, Shibboleth and SimpleSamlphp
- Integrates with COmanage via VOOT (based on OpenSocial)
- SURFnet is working with Grouper on SCIM support

OpenConext


Overview
Identity Provider
SAML2 IdP
Web Portal
Gadget
OpenSocial Container
Conext Engine
Grouper
TBD
TBD
JANUS
OpenSocial Rest
Group Management
Attribute Management
Virtual Organizations
Service Registry
OpenSocial Rest OAuth
SAML2 SP
SAML2 Metadata
Service Provider

SURFteams



SURFNET SURFteams

SURFteams — Welcome Benjamin Oshrin | Logout | Help

SURFconext Teams | Public Teams

search team

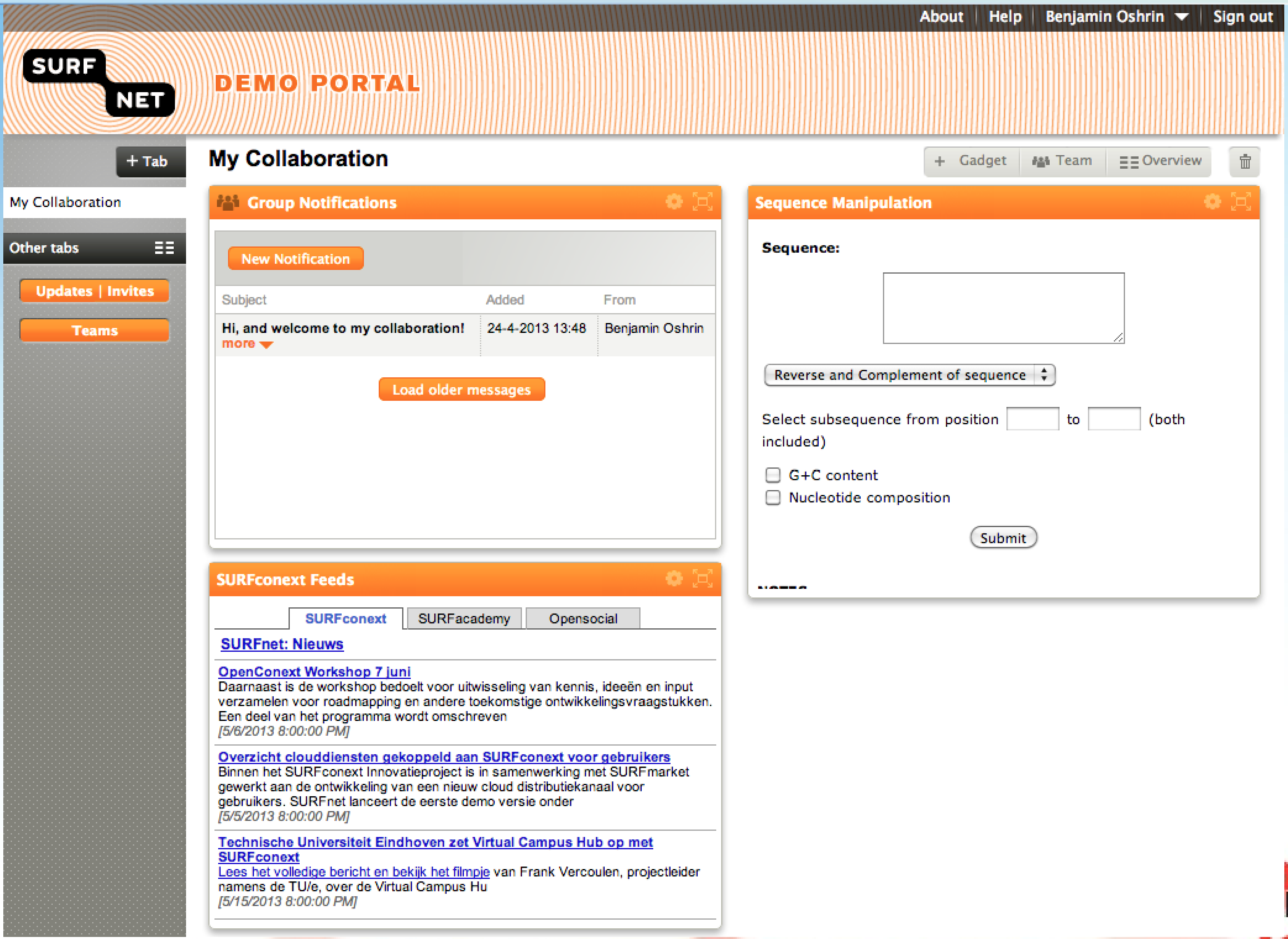
1 | 2 | 3 | 4 | 5 next ▶ last ▶▶

Add Team

Team	Description	Source
1234 test		nl:surfnet:diensten
123 test	bblaat	nl:surfnet:diensten
1337 Team	Test-team, aangemaakt op workshop 2011-11-17	nl:surfnet:diensten
2013 Internet2 demo		nl:surfnet:diensten
25mei2011SURFmedia	SURFmedia train de trainer workshop 25 mei 2011	nl:surfnet:diensten
3TU Datacentrum	Team met twee guestaccounts	nl:surfnet:diensten
3TU Identity Management	de 3TU groep waarmee we het Identity Management realiseren	nl:surfnet:diensten
4FFen test	team voor de poc met 4 ff	nl:surfnet:diensten
5 maart	Test 5 maart, edit?	nl:surfnet:diensten
5 maart jfartssurfnet	5 maart test Owner: jfartssurfnet	nl:surfnet:diensten

SURFnet bv   Radboudkwartier 273   Postbus 19035   3501 DA Utrecht   For questions email: help@surfteams.nl   Terms of Service   Copyright

SURFportal



My Collaboration

Group Notifications

Subject	Added	From
Hi, and welcome to my collaboration! more	24-4-2013 13:48	Benjamin Oshrin

SURFconext Feeds

SURFnet: Nieuws

OpenConext Workshop 7 juni
Daarnaast is de workshop bedoelt voor uitwisseling van kennis, ideeën en input verzamelen voor roadmapping en andere toekomstige ontwikkelingsvraagstukken. Een deel van het programma wordt omschreven
[5/6/2013 8:00:00 PM]

Overzicht clouddiensten gekoppeld aan SURFconext voor gebruikers
Binnen het SURFconext Innovatieproject is in samenwerking met SURFmarket gewerkt aan de ontwikkeling van een nieuw cloud distributiekanaal voor gebruikers. SURFnet lanceert de eerste demo versie onder
[5/5/2013 8:00:00 PM]

Technische Universiteit Eindhoven zet Virtual Campus Hub op met SURFconext
Lees het volledige bericht en bekijk het filmpje van Frank Vercoulen, projectleider namens de TU/e, over de Virtual Campus Hu
[5/15/2013 8:00:00 PM]

Sequence Manipulation

Sequence:

Reverse and Complement of sequence

Select subsequence from position ____ to ____ (both included)

□ G+C content
□ Nucleotide composition

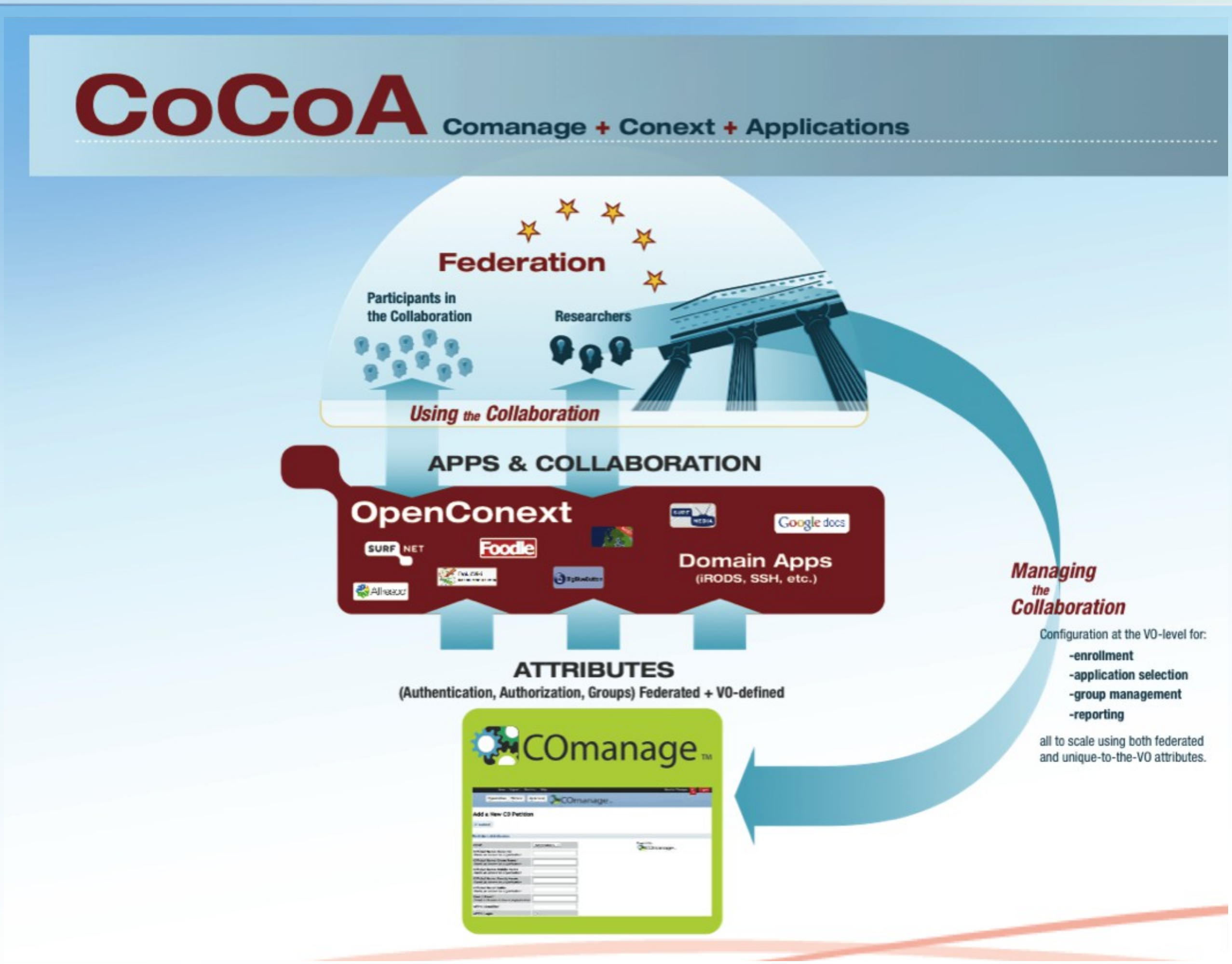
Applications:

Domestication & Integration

Applications

- General Purpose Collaboration Applications
  - Wikis, mailing lists, calendaring, conferencing, etc
- Domain-Specific Applications
- Domestication & Integration
  - Authentication externalized?
  - LDAP aware?
  - Provisionable?
  - Open Source vs Commercial vs Home Grown vs Cloud

CoCoA



Configuration at the VO-level for:

- -enrollment
- -application selection
- -group management
- -reporting

all to scale using both federated and unique-to-the-VO attributes.

Deployment Scenarios

- Central IT, for locally hosted smaller VOs
- VO IT, for larger VOs that run their own infrastructure
- Hosted service, especially for smaller/informal/transient VOs
- Use only the pieces you need
  - COmanage Registry
  - OpenConext
  - Grouper
  - LDAP Server
  - Shibboleth SP
  - Social2SAML Gateway
  - Applications

Status and Roadmap

- In Summary: Approaching Early Adopter
- COmanage Registry v0.8 RSN
  - More core features in next releases
  - Review scalability and UX issues for large collaborations
  - Details in JIRA
    - https://bugs.internet2.edu/jira/browse/CO
- Integration with OpenConext demonstrated, still provisional
- Looking for real world use cases willing to be Early Adopters

More Information

- COmanage Wiki Space
  - https://spaces.internet2.edu/display/COmanage
- OpenConext
  - http://www.openconext.org
- CoCoA White Paper
  - http://tinyurl.com/973njy7