VO con Grouper e COmanage

COmanage
(Collaborative Organization Management)

a cura del Gruppo di lavoro VOs del CTS

Roberta Cantaroni - Università di Modena e Reggio Emilia

Cos'è COmanage

COmanage e' un progetto di Internet2 per la creazione di una piattaforma per la collaborazione (Collaboration Management Platform – CMP).

L'obiettivo di COmanage è quello di semplificare la complessità della gestione delle identità di una Collaborative Organization (CO) sfruttando l'informazione delle singole home-institutions tramite Shibboleth Federated SSO e Grouper.
Si propone di fornire autenticazione e autorizzazione (gruppi, privilegi, etc) per l'accesso ad applicazioni "domesticated" quali Mediawiki, Subversion, Sympa, …

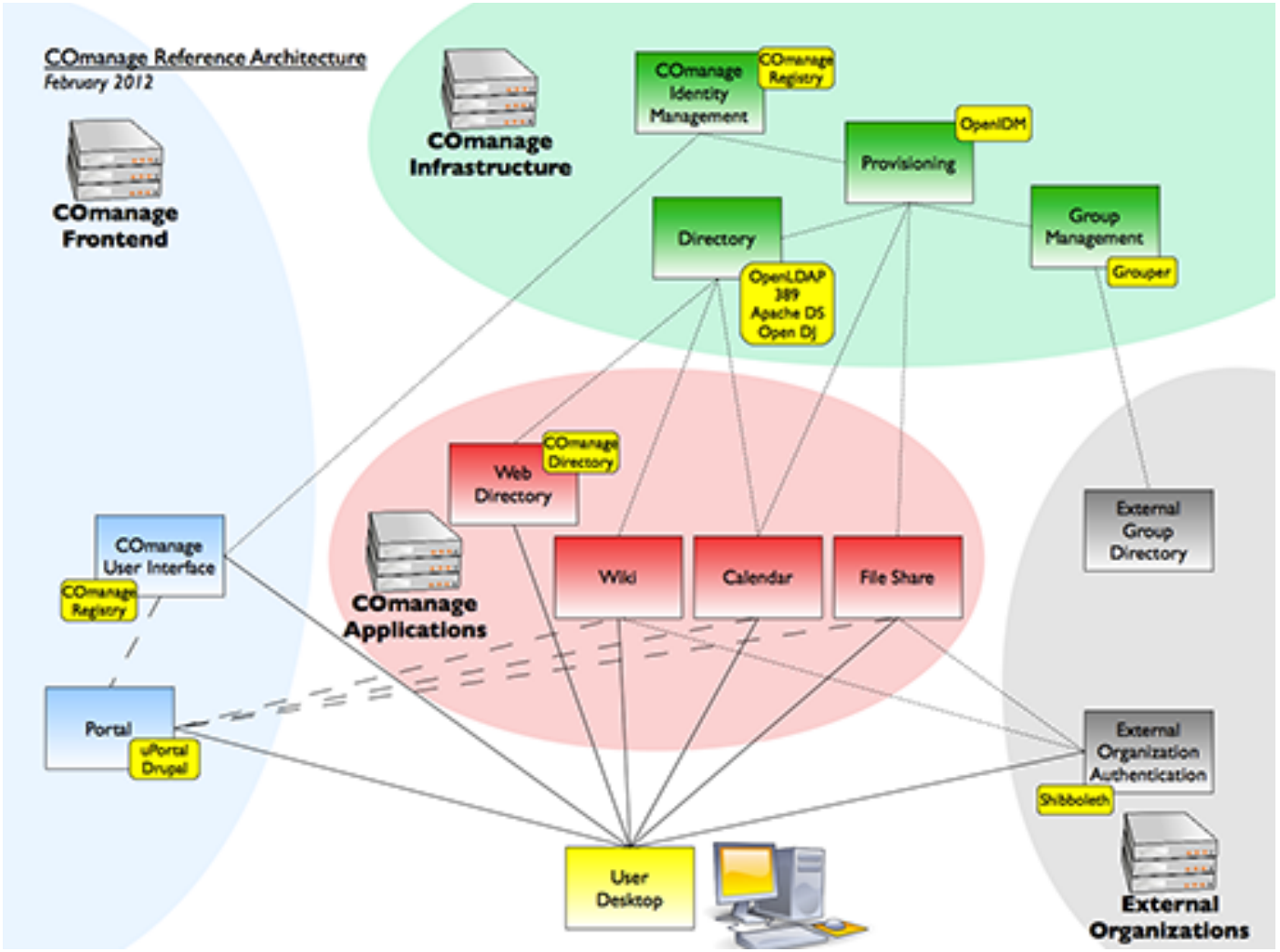
Funzionalità

- Gestione delle COs:
  - Creazione/rimozione di CO e COU (CO Unit)
- Gestione dei membri di una CO:
  - Invito/Inserimento/rimozione di un utente in una data CO
  - Definizione degli enrollment flows
  - Petitions
- Attribute authority:
  - Provisioning degli attributi di membership degli utenti

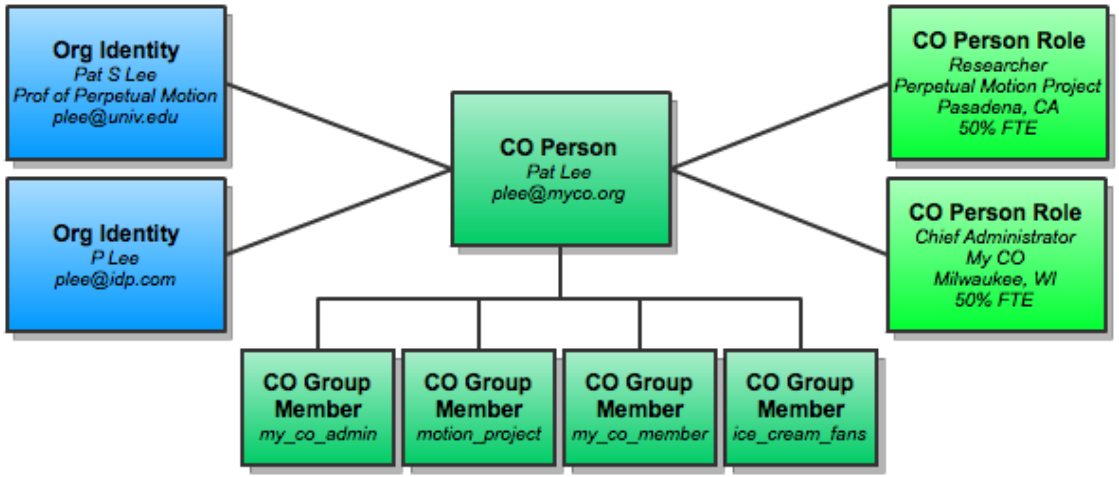
Componenti

- Software: Php, Mysql o Postgres, CakePHP, Apache
- Comanage Registry (versione 0.7)
  - Creazione CO e COu
  - Definizione delle identità, popolamento di una CO mediante invito o definizione di procedure ad hoc (enrollment flows, petitions)
- Comanage Directory (versione 0.1)
  - Ricerca degli utenti in ldap

Architettura (feb. 2012)



Registry Data Model



CO

collezione virtuale di persone che provengono da istituzioni reali e che collaborano insieme attraverso l'uso di servizi online

Organizational Identity

descrive la relazione della persona con la sua istituzione reale (ad esempio l'Università), possiede gli attributi forniti dal suo IdP

CO Person e COU Person

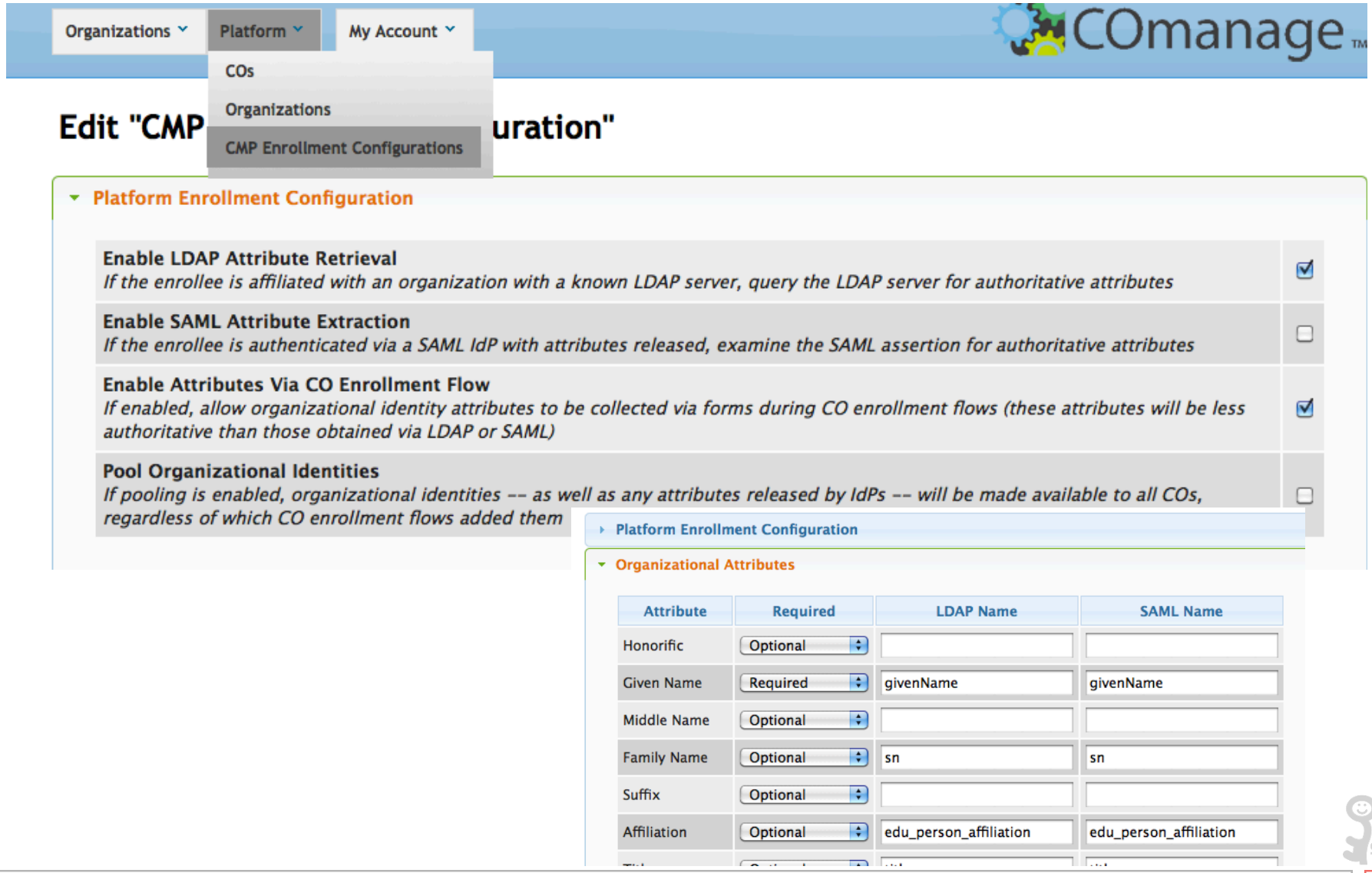
descrive la relazione della persona con la sua CO o COu, possiede ulteriori attributi assegnati dalla CO

Una persona può avere può avere *in un determinato momento* più di una relazione con la sua CO (***CO Person Role)***.

Accessi in Registry

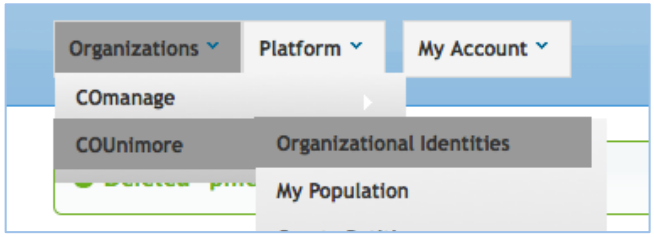
- **Registry Admin** (add-remove person to Registry, edit CO, …)
- **CO Admin** (create CO group/role, add-remove person from CO group/role, …)
- **CO Participant** (login to CO portal, login to CO application)
- **Guest** (view CO public content)
- **Sys Admin** (application upgrades, os upgrades, backups, …)

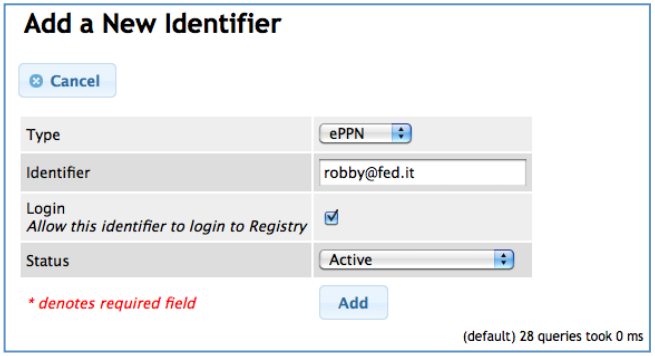
CMP Enrollment Configuration



Enrollment - 1

Il CO Admin può creare una *Organizational Identity* assegnando gli identificatori (**email** per l'invito, **eppn** per il login, …)



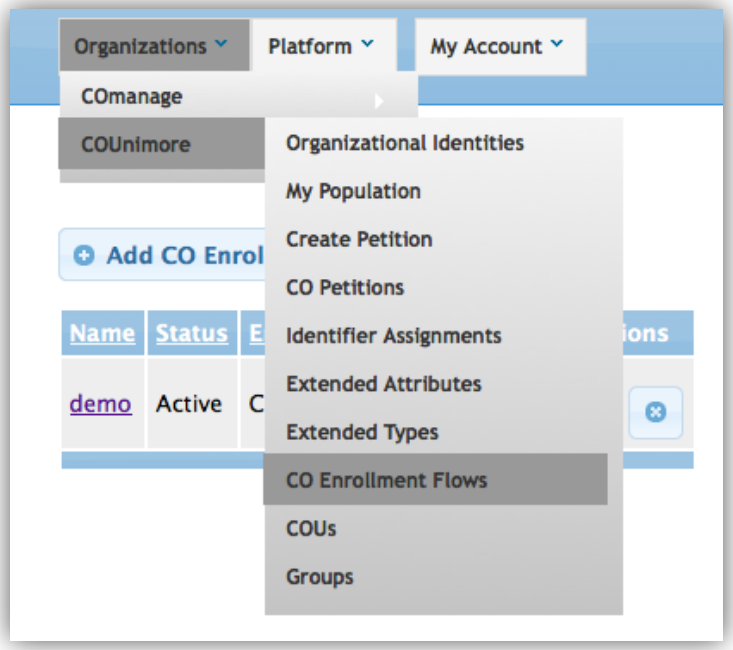


Default: invito via email

Enrollment - 2

Il CO Admin definisce *uno o più* **Enrollment Flows** per la CO definendo gli attributi che saranno richiesti

L'Enrollment avviene con l'avvio di una **Petition**

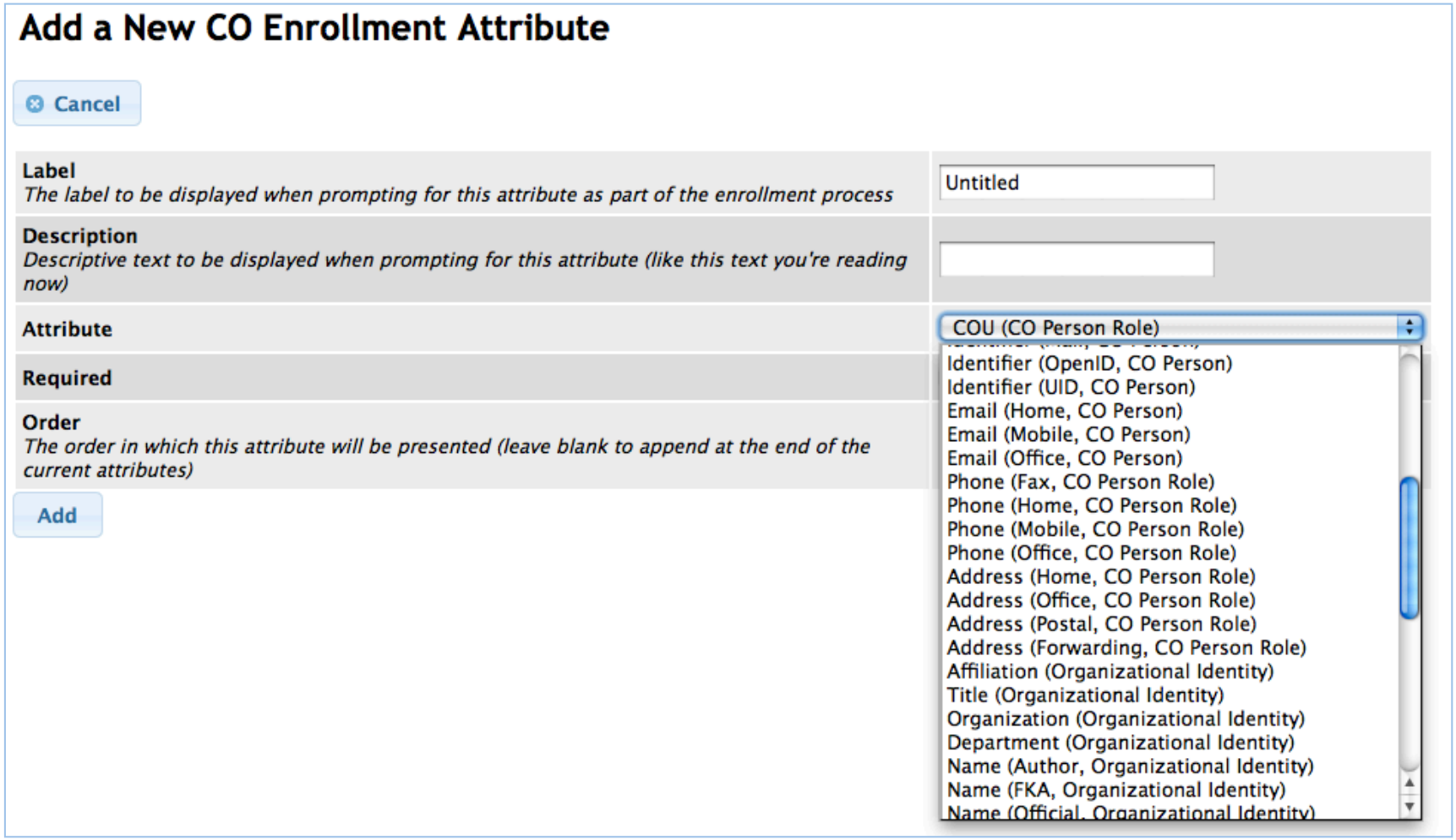


Enrollment - 3

Add a New CO Enrollment Flow

Name	Untitled
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*	

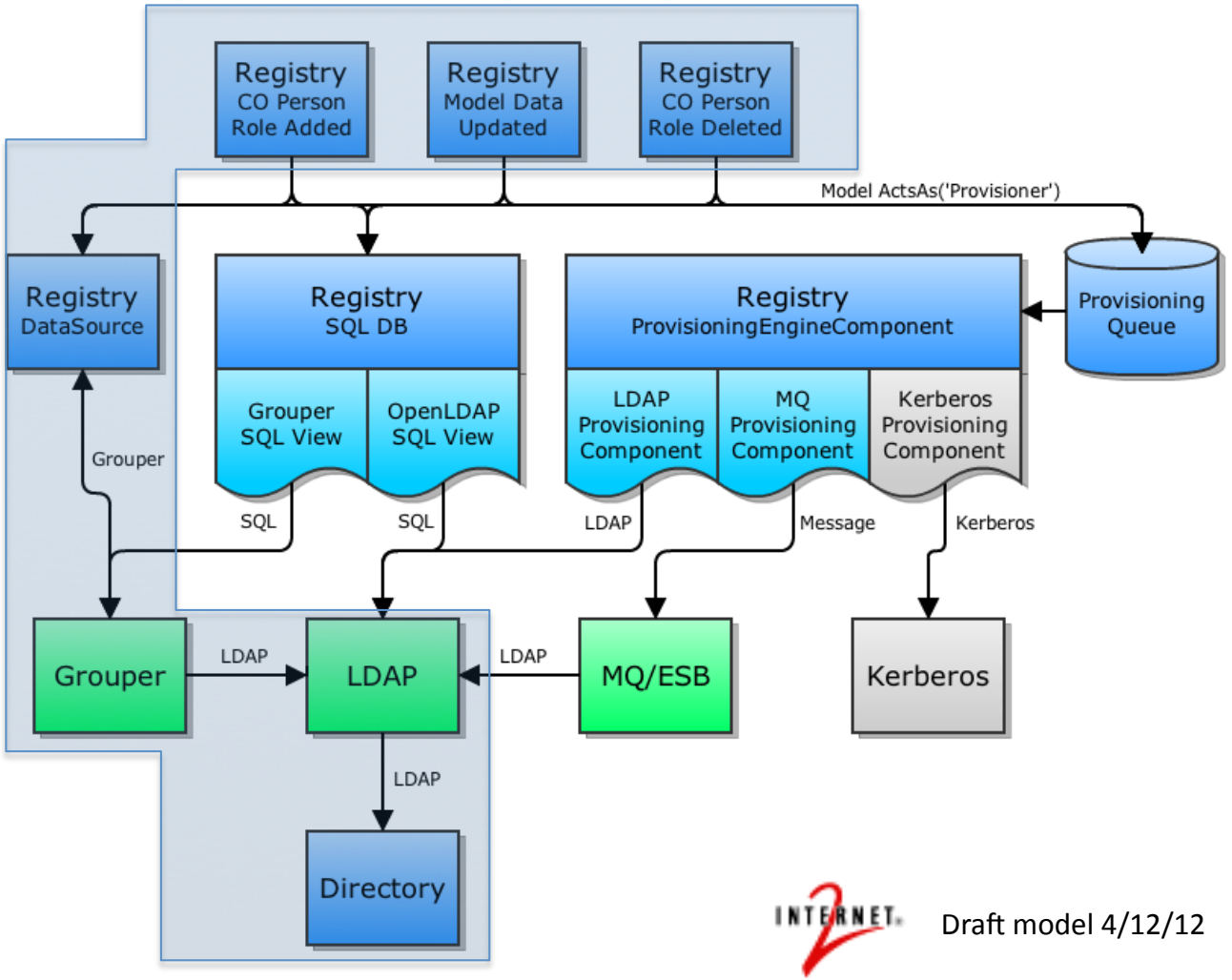
Enrollment - 4



Esempi di Enrollment Flows

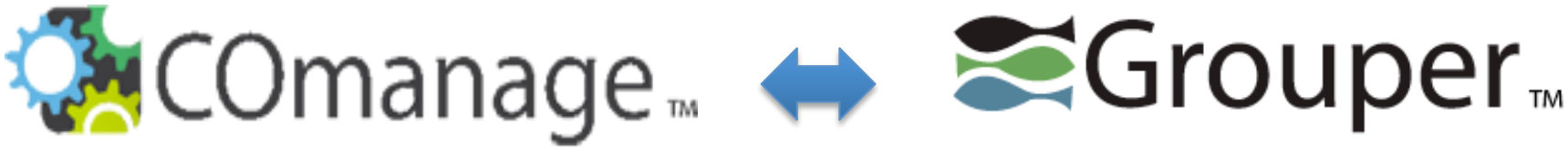
- Conscription:
  - viene aggiunta una CO person con approvazione di CO admin ma senza conferma utente
- Invitation:
  - approvazione di CO admin e conferma utente
- Self-signup:
  - non richiede alcuna approvazione
- Account linking:
  - la persona esiste già nella CO e vuole aggiungere una ulteriore organizational identity

Provisioning from Registry



Draft model 4/12/12

Attributi di membership – provisioning su Grouper

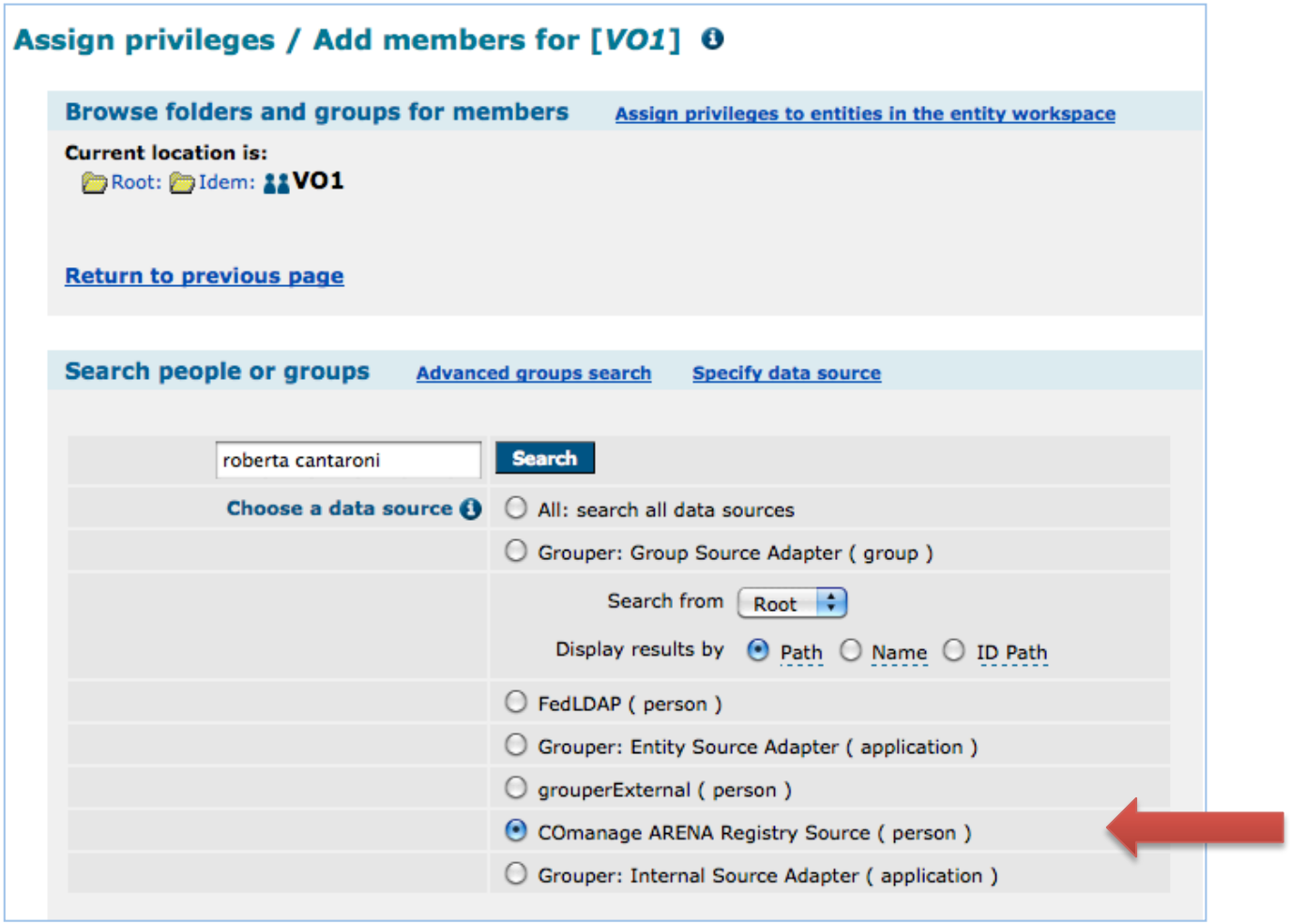


COmanage Registry può essere collegato con Grouper in 2 modi

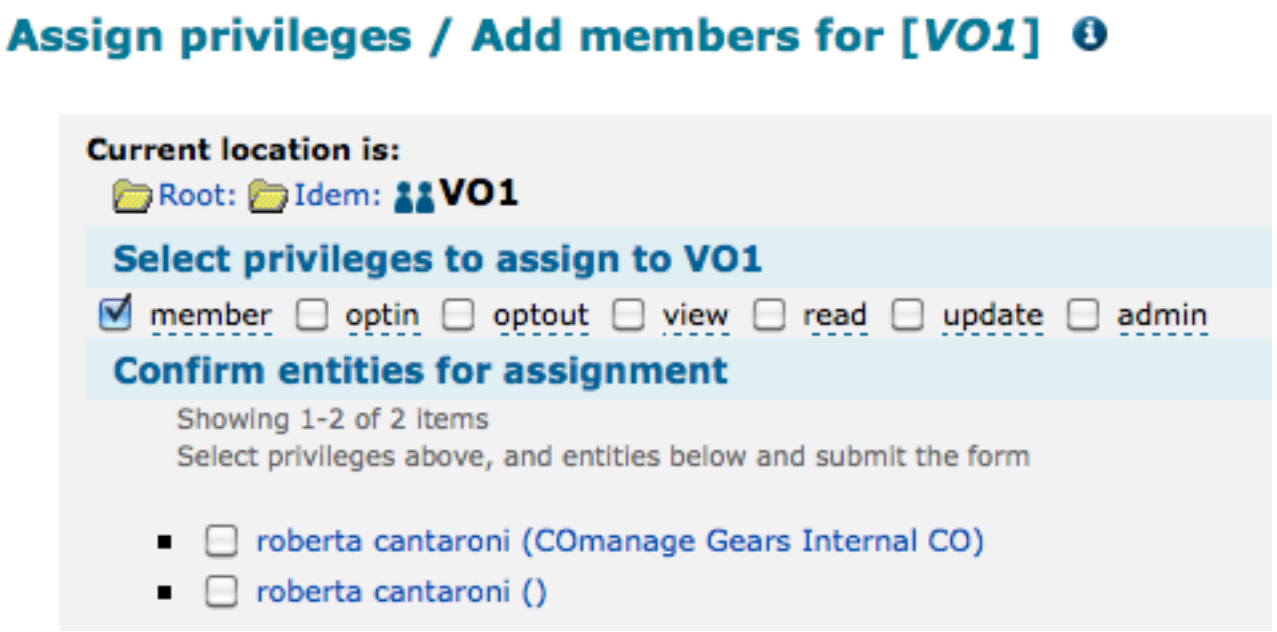
- CASO 1:
  - Grouper usa Registry come Subject Source

- CASO 2:
  - Grouper vede i gruppi definiti all'interno di una CO

CASO 1: Registry come Subject Source di Grouper



CASO 1: Registry come Subject Source di Grouper



Gli attributi Grouper di un subject trovato in Registry

lfname	cantaroni,roberta
loginid1	null
loginid2	null
loginid3	null
loginid4	null
loginid5	null
email1	robby@unimore.it
email2	
email3	
email4	
email5	
Entity type	person
ID	1

Provisioning via Grouper-PSP

CASO 2: Gruppi di Comanage in Grouper

In Grouper i gruppi delle CO compaiono sotto uno specifico stem definito in sources.xml (default Reference:ComanageDataSource)


```
# Reference, groups, fed.it
dn: ou=Reference,ou=groups,dc=fed,dc=it
ou: Reference
objectClass: organizationalUnit
objectClass: top

# Reference:COmanageDataSource, groups, fed.it
dn: ou=Reference:COmanageDataSource,ou=groups,dc=fed,dc=it
ou: COmanageDataSource
ou: Reference:COmanageDataSource
objectClass: organizationalUnit
objectClass: top
```

Riferimenti

COmanage home page:

- http://www.internet2.edu/comanage

Wiki:

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

Ringraziamenti

- **Danilo Crecchia** – Università di Modena e Reggio Emilia (membro del CTS-IDEM)
- **Francesco Malvezzi** – Università di Modena e Reggio Emilia

e … ovviamente

- **Raffaele Conte** – CNR