

VO con Grouper e COmanage

**COmanage**

**(Collaborative Organization Management)**

a cura del Gruppo di lavoro VOs del CTS

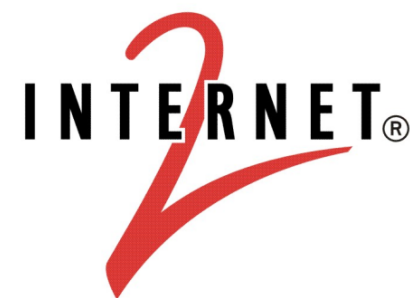
Roberta Cantaroni - Università di Modena e Reggio Emilia

# 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, ...



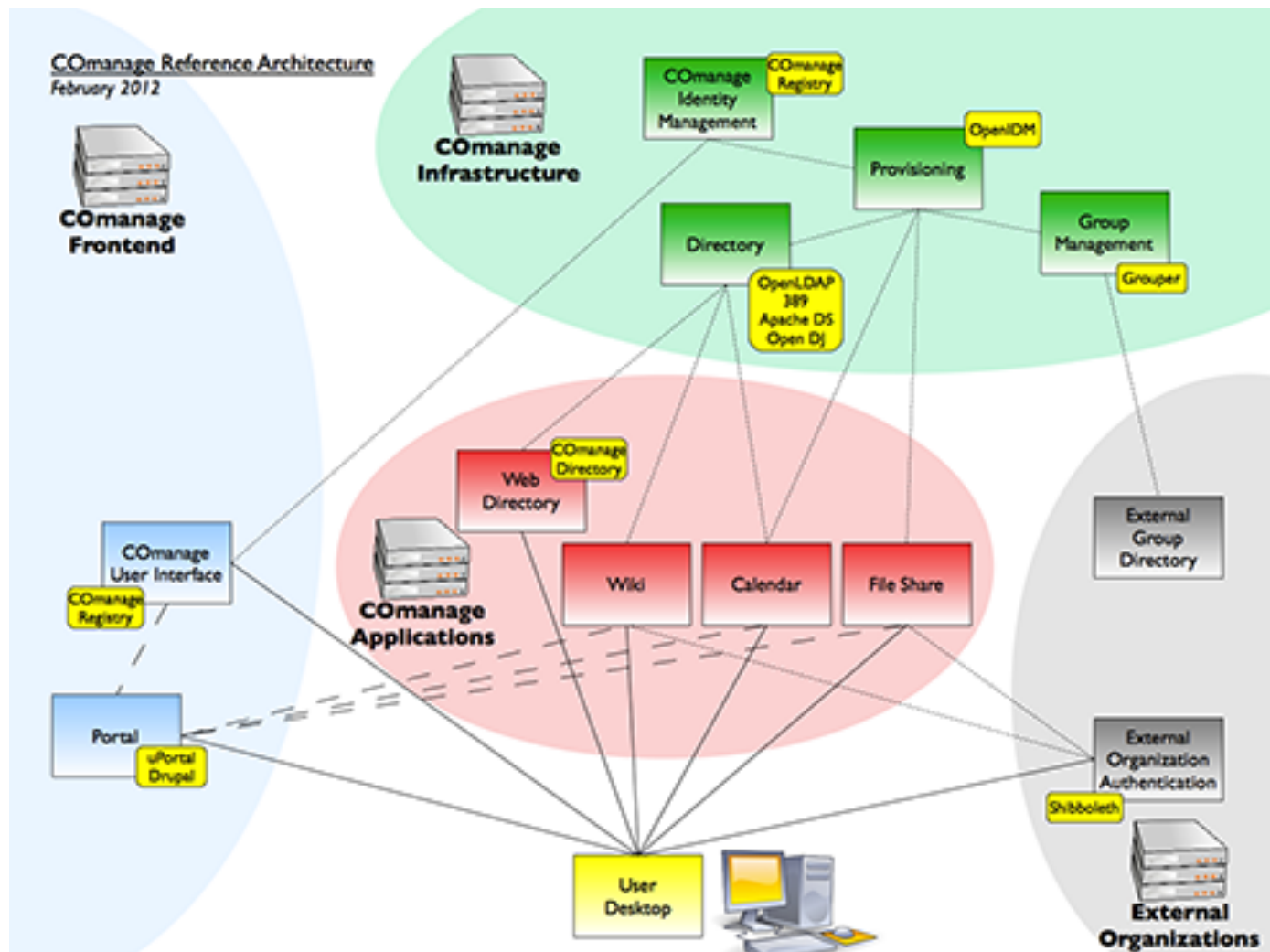
# Funzionalità

- 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

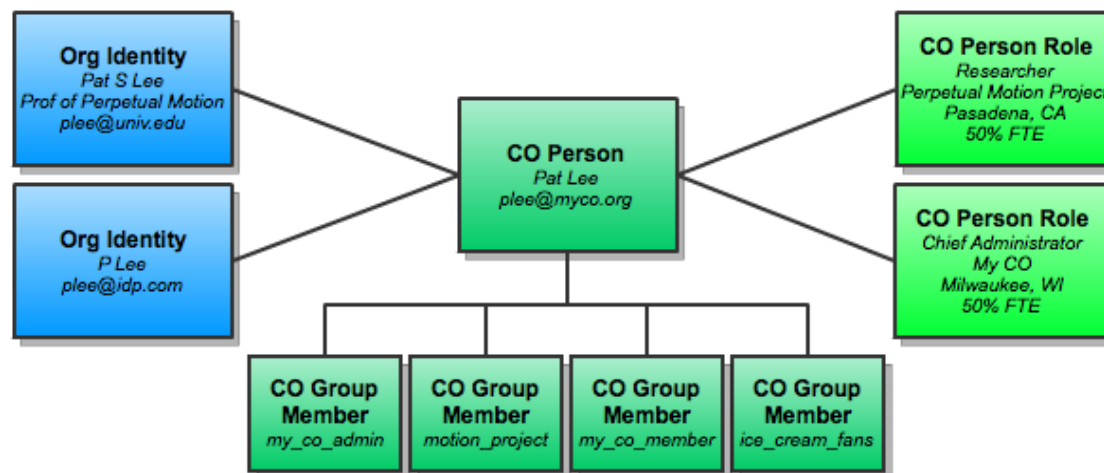
# Architettura (feb. 2012)



INTERNET



# 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 *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

Organizations Platform My Account

COs  
Organizations  
CMP Enrollment Configurations

## Edit "CMP Enrollment Configuration"

Platform Enrollment Configuration

- Enable LDAP Attribute Retrieval**  
*If the enrollee is affiliated with an organization with a known LDAP server, query the LDAP server for authoritative attributes*
- Enable SAML Attribute Extraction**  
*If the enrollee is authenticated via a SAML IdP with attributes released, examine the SAML assertion for authoritative attributes*
- Enable Attributes Via CO Enrollment Flow**  
*If enabled, allow organizational identity attributes to be collected via forms during CO enrollment flows (these attributes will be less authoritative than those obtained via LDAP or SAML)*
- Pool Organizational Identities**  
*If pooling is enabled, organizational identities -- as well as any attributes released by IdPs -- will be made available to all COs, regardless of which CO enrollment flows added them*

Platform Enrollment Configuration

Organizational Attributes

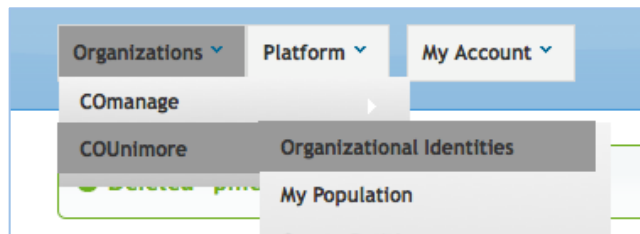
Attribute	Required	LDAP Name	SAML Name
Honorific	Optional		
Given Name	Required	givenName	givenName
Middle Name	Optional		
Family Name	Optional	sn	sn
Suffix	Optional		
Affiliation	Optional	edu_person_affiliation	edu_person_affiliation





# Enrollment - 1

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



**Add a New Organizational Identity**

**Name and Affiliation**

Honorific (Dr, Hon, etc)	<input type="text"/>
Given Name*	<input type="text"/>
Middle Name	<input type="text"/>
Family Name	<input type="text"/>
Suffix (Jr, III, etc)	<input type="text"/>
Affiliation*	<input type="text" value="Member"/>
Title	<input type="text"/>
Organization	<input type="text"/>
Department	<input type="text"/>

\* denotes required field

(default) 20 queries took 0 ms

**Add a New Identifier**

Type	<input type="text" value="ePPN"/>
Identifier	<input type="text" value="robby@fed.it"/>
Login Allow this identifier to login to Registry	<input checked="" type="checkbox"/>
Status	<input type="text" value="Active"/>

\* denotes required field

(default) 28 queries took 0 ms

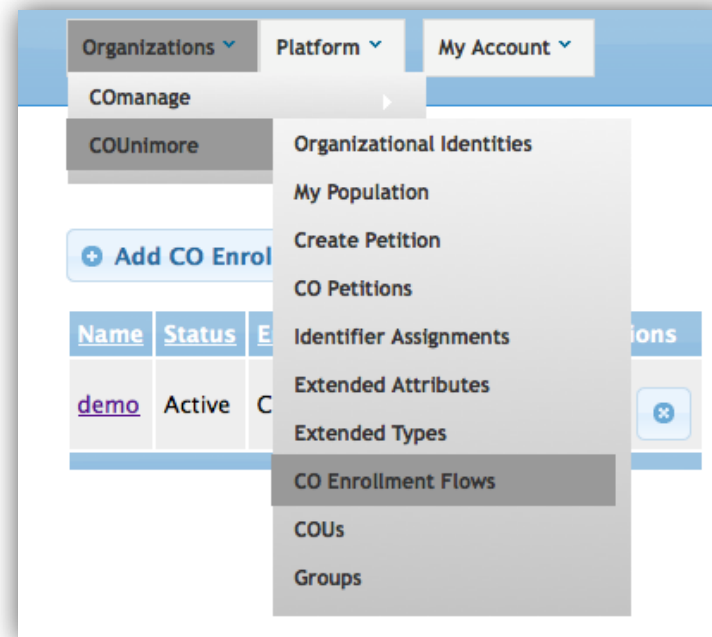
Default: invito via email



# 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

<b>Name</b>	Untitled
<b>Status*</b>	Active
<b>Enrollment Authorization</b> <i>Authorization required to execute this enrollment flow, see <a href="#">Enrollment Authorization</a> for details</i>	CO or COU Admin
<b>Identity Matching</b> <i>Identity Matching policy for this enrollment flow, see <a href="#">Identity Matching</a> for details</i>	Advisory
<b>Require Approval For Enrollment</b> <i>If administrator approval is required, a member of the appropriate <code>admin.approvers</code> group must approve the enrollment</i>	<input type="checkbox"/>
<b>Require Confirmation of Email</b> <i>Confirm email addresses provided by sending a confirmation URL to the address</i>	<input type="checkbox"/>
<b>Require Authentication</b> <i>Require enrollee to authenticate in order to complete their enrollment</i>	<input type="checkbox"/>
<b>Early Provisioning Executable</b> <i>(Need for this TBD)</i>	
<b>Provisioning Executable</b> <i>Executable to call to initiate user provisioning</i>	
<b>Notify On Early Provisioning</b> <i>Email address to notify upon execution of early provisioning</i>	
<b>Notify On Provisioning</b> <i>Email address to notify upon execution of provisioning</i>	
<b>Notify On Active Status</b> <i>Email address to notify upon status being set to active</i>	



# Enrollment - 4

## Add a New CO Enrollment Attribute

Cancel

**Label**

*The label to be displayed when prompting for this attribute as part of the enrollment process*

Untitled

**Description**

*Descriptive text to be displayed when prompting for this attribute (like this text you're reading now)*

**Attribute**

COU (CO Person Role)

**Required**

**Order**

*The order in which this attribute will be presented (leave blank to append at the end of the current attributes)*

Add

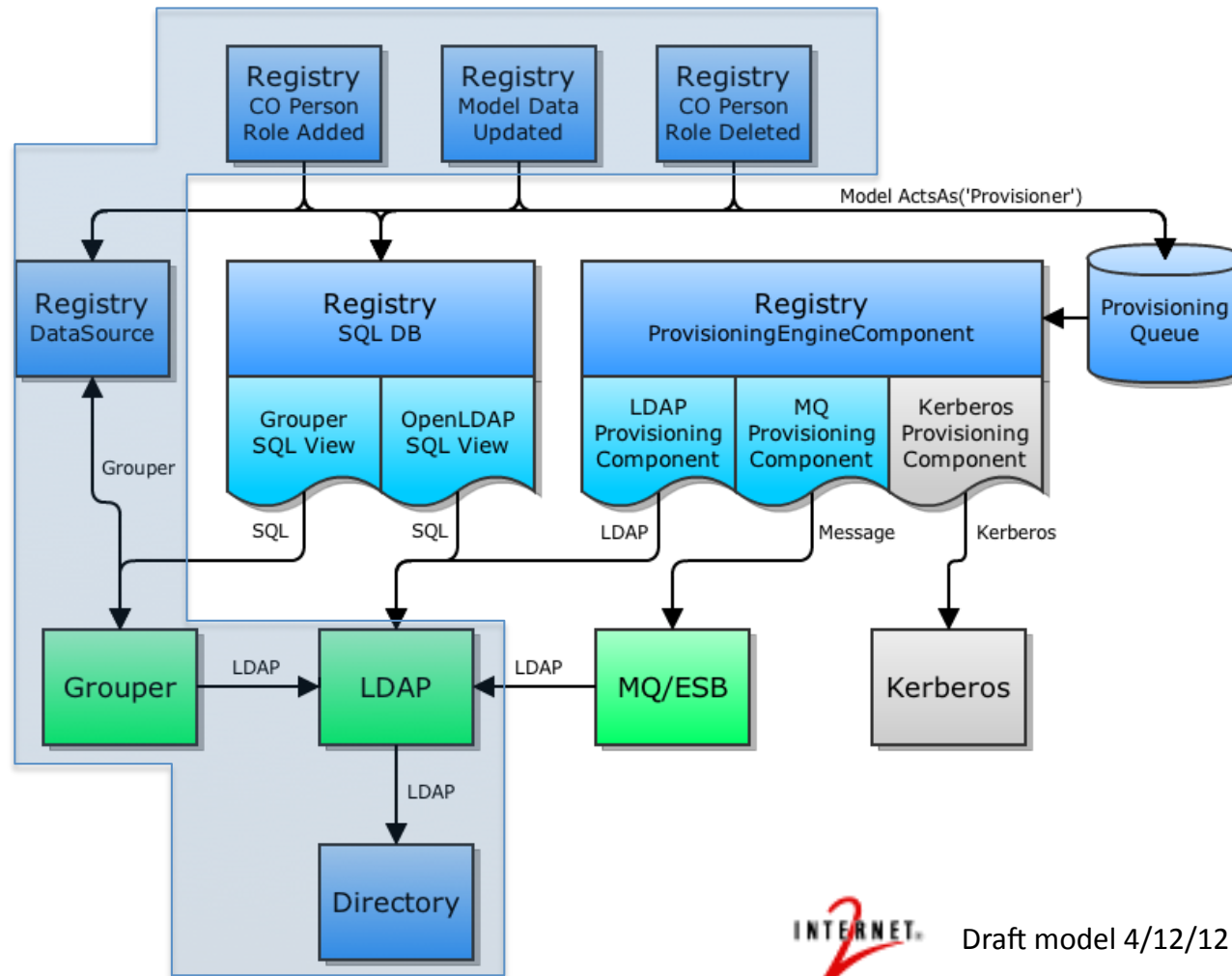
- Identifier (OpenID, CO Person)
- Identifier (UID, CO Person)
- Email (Home, CO Person)
- Email (Mobile, CO Person)
- Email (Office, CO Person)
- Phone (Fax, CO Person Role)
- Phone (Home, CO Person Role)
- Phone (Mobile, CO Person Role)
- Phone (Office, CO Person Role)
- Address (Home, CO Person Role)
- Address (Office, CO Person Role)
- Address (Postal, CO Person Role)
- Address (Forwarding, CO Person Role)
- Affiliation (Organizational Identity)
- Title (Organizational Identity)
- Organization (Organizational Identity)
- Department (Organizational Identity)
- Name (Author, Organizational Identity)
- Name (FKA, Organizational Identity)
- Name (Official, Organizational Identity)



# 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

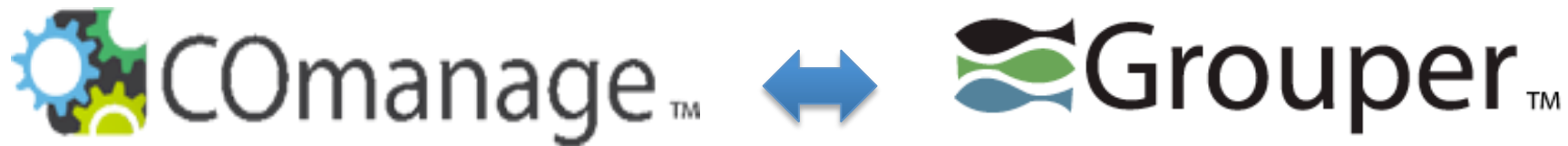
# Provisioning from Registry



INTERNET. 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

**Assign privileges / Add members for [VO1]** ⓘ

**Browse folders and groups for members** [Assign privileges to entities in the entity workspace](#)

**Current location is:**  
📁 Root: 📁 Idem: 👤 VO1


[Return to previous page](#)

**Search people or groups** [Advanced groups search](#) [Specify data source](#)

**Search**

**Choose a data source** ⓘ

- All: search all data sources
- Grouper: Group Source Adapter ( group )
- Search from
- Display results by  Path  Name  ID Path
- FedLDAP ( person )
- Grouper: Entity Source Adapter ( application )
- grouperExternal ( person )
- COmanage ARENA Registry Source ( person )
- Grouper: Internal Source Adapter ( application )





# CASO 1: Registry come Subject Source di Grouper

## Assign privileges / Add members for [VO1] ⓘ

Current location is:

📁 Root: 📁 Idem: 👤 VO1

### Select privileges to assign to VO1

member  optin  optout  view  read  update  admin

### Confirm entities for assignment

Showing 1-2 of 2 Items

Select privileges above, and entities below and submit the form

- roberta cantaroni (COmanage Gears Internal CO)
- roberta cantaroni ()



# Gli attributi Grouper di un subject trovato in Registry

<b>lname</b>	cantaroni,roberta
<b>loginid1</b>	null
<b>loginid2</b>	null
<b>loginid3</b>	null
<b>loginid4</b>	null
<b>loginid5</b>	null
<b>email1</b>	robby@unimore.it
<b>email2</b>	
<b>email3</b>	
<b>email4</b>	
<b>email5</b>	
<b>Entity type</b>	person
<b>ID</b>	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)

## Browse groups hierarchy ⓘ

You can look for groups throughout the hierarchy.  
(You might not be able to see some groups if you lack appropriate privileges.)

### Browse or list groups ⓘ

Current location is:

📁 Root: 📁 Reference

Showing 1-1 of 1 items

📁 CManageDataSource



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

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

### Search groups

[Advanced groups search](#)

Search from

Display results by  Path  Name  ID Path



# 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

