

# Progetto IdP in cloud

IdP provisioning on-demand

# Premesse

- la diffusione della gestione d'identità federata è ostacolata
  - non facile attribuzione di competenza all'interno di una organizzazione della gestione delle identità del personale
  - non facile comprensione dei benefici che da essa ne derivano
- infine
  - complessità tecnologica

## Perchè la comunità della ricerca biomedica

- Nel 2005 è stata siglata la prima Convenzione Quadro tra Ministero della Salute e GARR (durata biennale)
- Nel 2009 è stato siglato un Accordo di Programma (durata triennale)
- Prolungato fino a dicembre 2014 l'Accordo di Programma attraverso un Atto Aggiuntivo

### Estensione della rete

- 43 sedi di IRCCS (Istituto di Ricerca a Carattere Scientifico)
- estensione a 2 sedi Ministero della Salute e alla sede Fondazione CNAO
- estensione 10 sedi Istituti Zooprofilattici Sperimentali

In totale oggi 55 sedi collegate su tutto il territorio nazionale



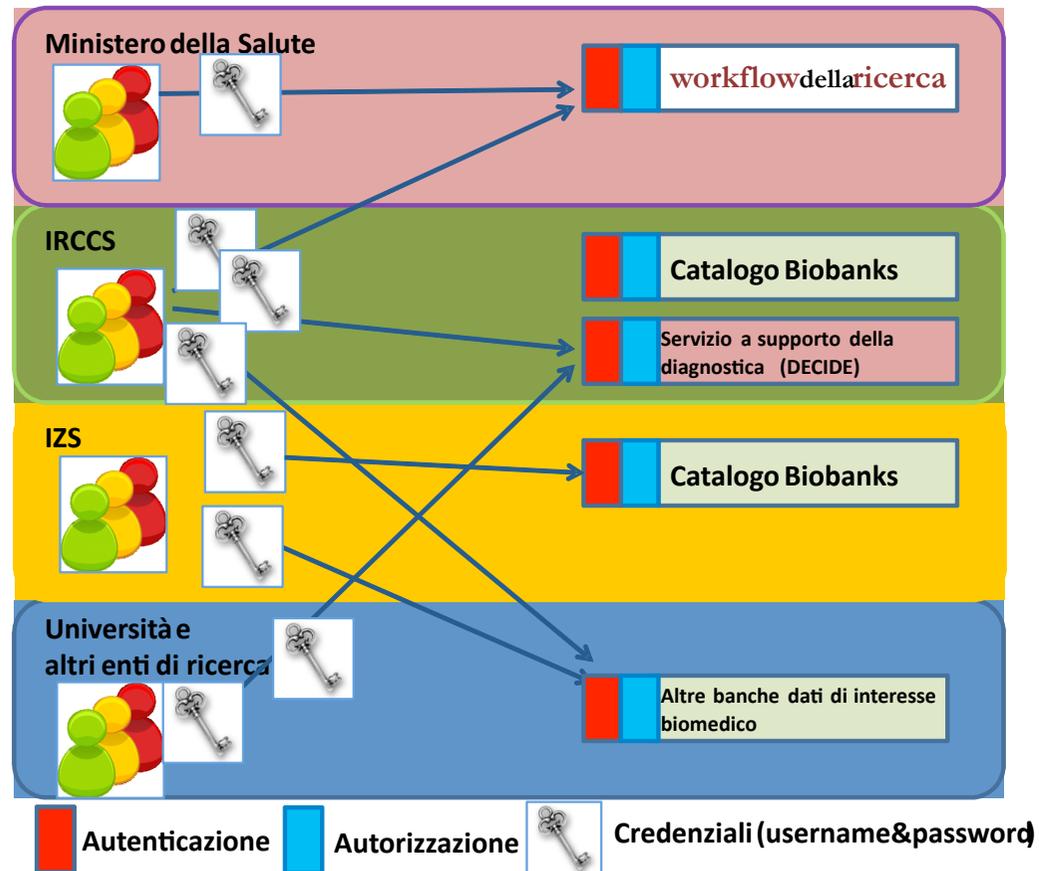
# Perchè IDEM per la comunità ricerca biomedica

- condivisione di applicazioni e strumenti fra gli istituti della comunità
- condivisione dei risultati della ricerca con regole trasparenti
- strumento flessibile per aggiungere nuove risorse e realizzare gruppi di lavoro in contesti di progetti di ricerca
- sicurezza nella gestione dei privilegi per accesso alle risorse

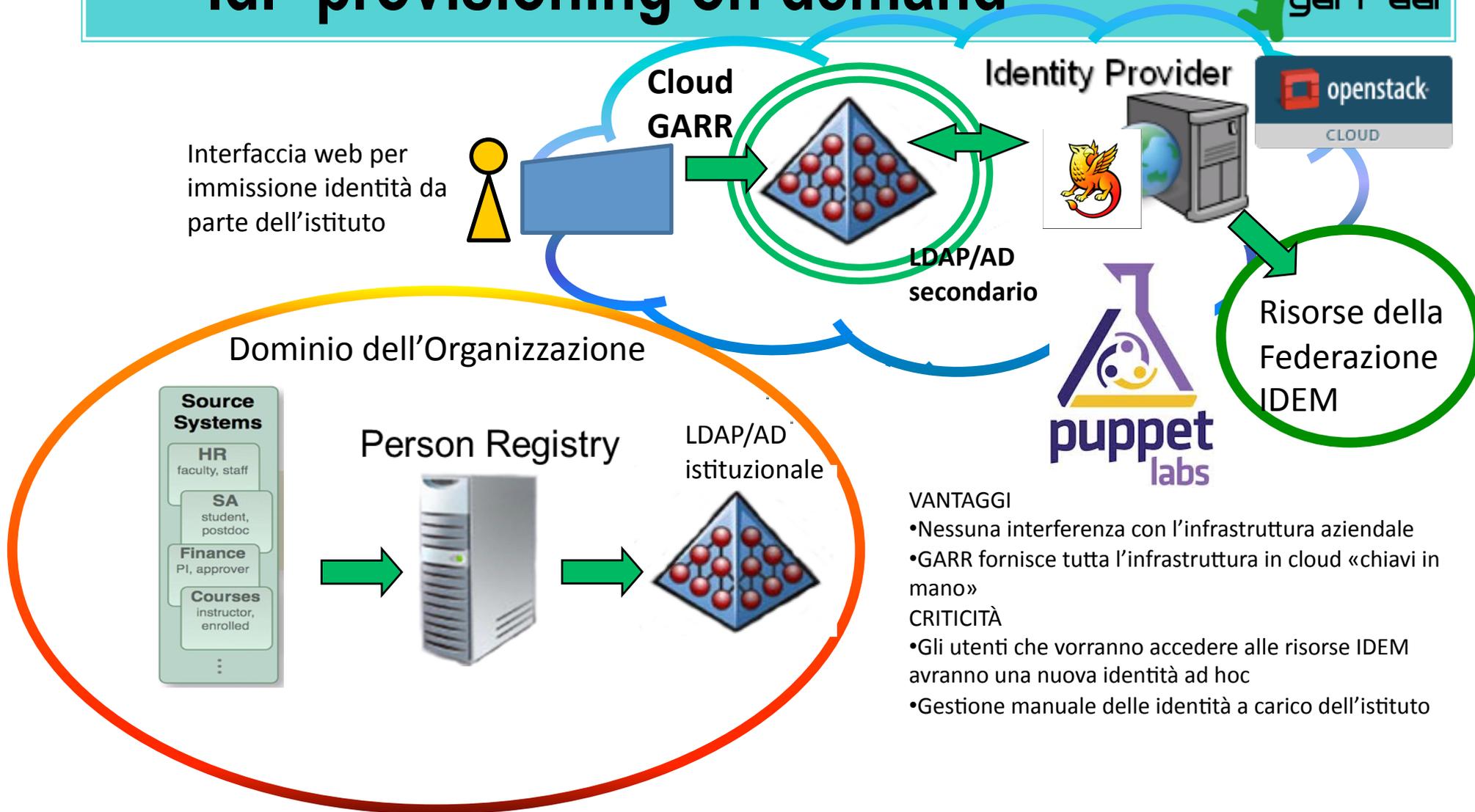


# Come favorisce la comunità ricerca biomedica

- Come possiamo facilitare e semplificare l'accesso alle risorse ?



# IdP provisioning on demand



## VANTAGGI

- Nessuna interferenza con l'infrastruttura aziendale
- GARR fornisce tutta l'infrastruttura in cloud «chiavi in mano»

## CRITICITÀ

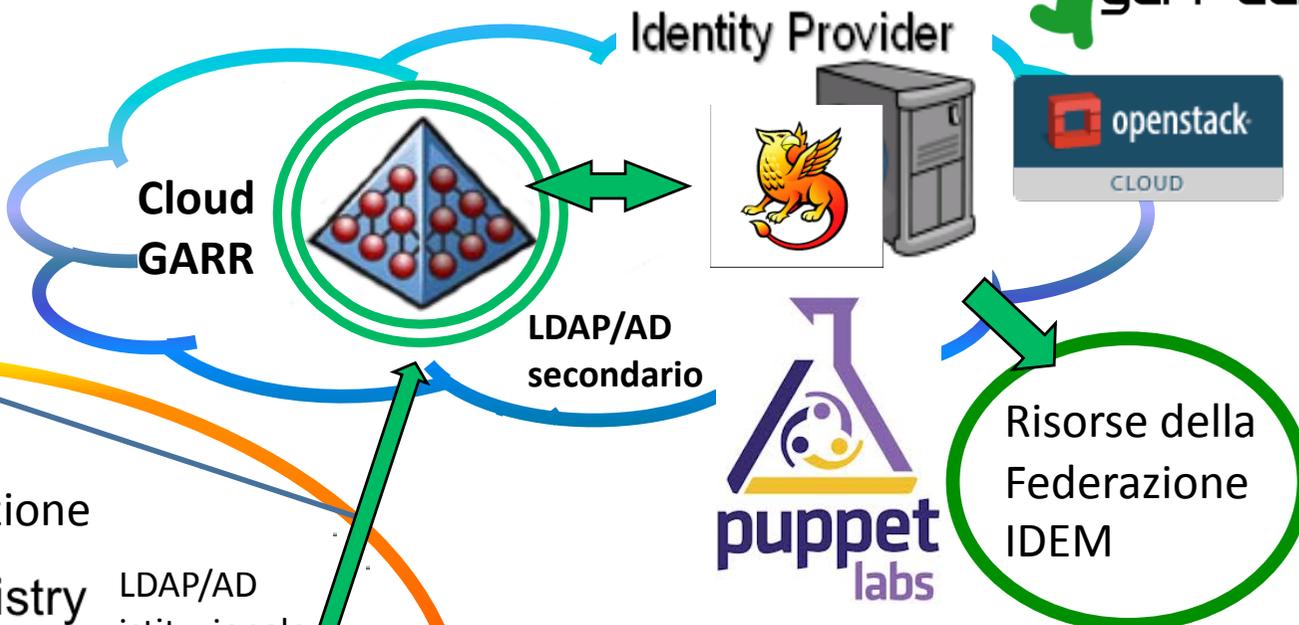
- Gli utenti che vorranno accedere alle risorse IDEM avranno una nuova identità ad hoc
- Gestione manuale delle identità a carico dell'istituto



# IdP provisioning on demand: soluzione intermedia



Sincronizzazione automatica su un canale sicuro



Dominio dell'Organizzazione

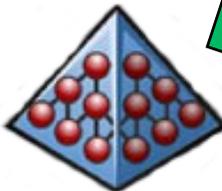
**Source Systems**

- HR**  
faculty, staff
- SA**  
student, postdoc
- Finance**  
PI, approver
- Courses**  
instructor, enrolled

Person Registry



LDAP/AD istituzionale



## VANTAGGI

- Nessuna interferenza con l'infrastruttura aziendale
- GARR fornisce tutta l'infrastruttura in cloud «chiavi in mano»
- Gli utenti che vorranno accedere alle risorse IDEM useranno la stessa identità istituzionale

## CRITICITÀ

- I dati personali basilari delle identità aziendali sono replicati nella cloud
- La procedura di sincronizzazione non è compresa nel progetto: richiede lavoro personalizzato per istituto



# Interfaccia WEB per Identity Management



Home | Purge caches | Show Cache

IDP Milano Test

schema search refresh info import export

dc=example, dc=com (3)

cn=admin

ou=groups (1)

ou=people (10)

uid=andrea

uid=cristiano

uid=fabio

uid=fulvio

uid=luca

uid=marco

uid=mario

uid=simon

uid=simone

uid=test

★ Create new entry here

★ Create new entry here

## Create Object

Server: IDP Milano Test Container: ou=people,dc=example,dc=com

Select a template for the creation process

Templates:

Identity Provider: Creazione nuovo utente

Default



1.2.3  
sourceforge

### IDP Milano Test

- schema search refresh info import export

- dc=example,dc=com (3)
  - cn=admin
- ou=groups (1)
- ou=people (10)
  - uid=andrea
  - uid=cristiano
  - uid=fabio
  - uid=fulvio
  - uid=luca
  - uid=marco
  - uid=mario
  - uid=simon
  - uid=simone
  - uid=test
- ★ Create new entry here
- ★ Create new entry here

## Create Object

Server: IDP Milano Test Container: ou=people,dc=example,dc=com  
Template: Identity Provider: Creazione nuovo utente (custom\_idpAccount)

### Identity Provider: Creazione nuovo utente (Step 1 of 1)

<b>Cognome</b> <small>alias, required</small>	<input type="text" value="*"/>
<b>Nome</b> <small>alias</small>	<input type="text"/>
<b>Nome Cognome</b>	<input type="text"/>
<b>Data di nascita</b>	<input type="text" value="YYYYmmdd"/>
<b>Provincia di nascita</b>	<input type="text"/>
<b>Codice fiscale</b>	<input type="text"/>
<b>Indirizzo</b>	<input type="text"/>
<b>Città</b>	<input type="text"/>
<b>Provincia</b> <small>alias</small>	<input type="text"/>
<b>Indirizzo e-mail (alla quale saranno inviate tutte le comunicazioni)</b> <small>alias</small>	<input type="text"/>
<b>Telefono 1</b> <small>alias</small>	<input type="text"/>
<b>Sezione/Divisione/Unità/Laboratorio in cui si svolgono le funzioni di operatore SSN</b> <small>alias</small>	<input type="text"/>
<b>Struttura con cui si ha un rapporto di lavoro/collaborazione al momento della registrazione</b> <small>alias</small>	<input type="text"/>
<b>Nome utente</b>	<input type="text" value="*"/>
<b>Password</b>	<input type="password"/>
	<input type="password" value="Encryption (confirm)"/>
	<input type="button" value="Check password..."/>



# Nulla cambia per la richiesta di adesione IDEM



## Richiesta di Adesione per la partecipazione in qualità di Membro

v1.2 del 23/02/2010

A<sup>1</sup>: Consortium GARR,  
Servizio GARR-IDEM  
Via dei Tizii, 6  
I 00185 Roma  
Tel +39 06 4962.2000  
Fax +39 06 4962 2044  
Email : idem@garr.it

Il sottoscritto .....  
(nome e cognome)

in qualità di legale rappresentante,

CHIEDE

per .....  
(denominazione dell'Organizzazione)

l'ammissione alla Federazione Italiana delle Università e degli Enti di Ricerca per l'Autenticazione e l'Auto-rizzazione denominata IDEM (di seguito ed in tutti i documenti "IDEM" oppure "Federazione") assumendosi le responsabilità che derivano dalla partecipazione.

Il sottoscritto in particolare dichiara:

1. di essere a conoscenza che l'adesione e la partecipazione alla Federazione sono soggette al *Regolamento della Federazione*, alle *Norme di Partecipazione*, alle *Specifiche tecniche*, alle *Specifiche tecniche per la compilazione e l'uso degli attributi* e a tutti i documenti riferiti nei precedenti. che



# Impatto

- Registrazione di nuove risorse in IDEM
- Il lavoro fatto rappresenta una opportunità in altri contesti
  - istituti di piccola/media grandezza che non hanno dipartimenti di Information & Technology al proprio interno
  - strutture inadeguate ad ospitare HW al proprio interno
  - ambiti progettuali nazionali e internazionali per i quali non percorribile con i tempi del progetto l'adesione alla Federazione IDEM

# Team GARR del progetto

- *Andrea Biancini*
- *Fabio Farina*
- *Marco Malavolti*
- *Pasquale Mandato*
- *Maria Laura Mantovani*
- *Barbara Monticini*
- *Luca Prete*
- *Sabrina Tomassini*
- *Cristiano Valli*
- *Simona Venuti*

