

**Science Gateway: dove l'utente comune  
tocca la Grid grazie all'identità federata**

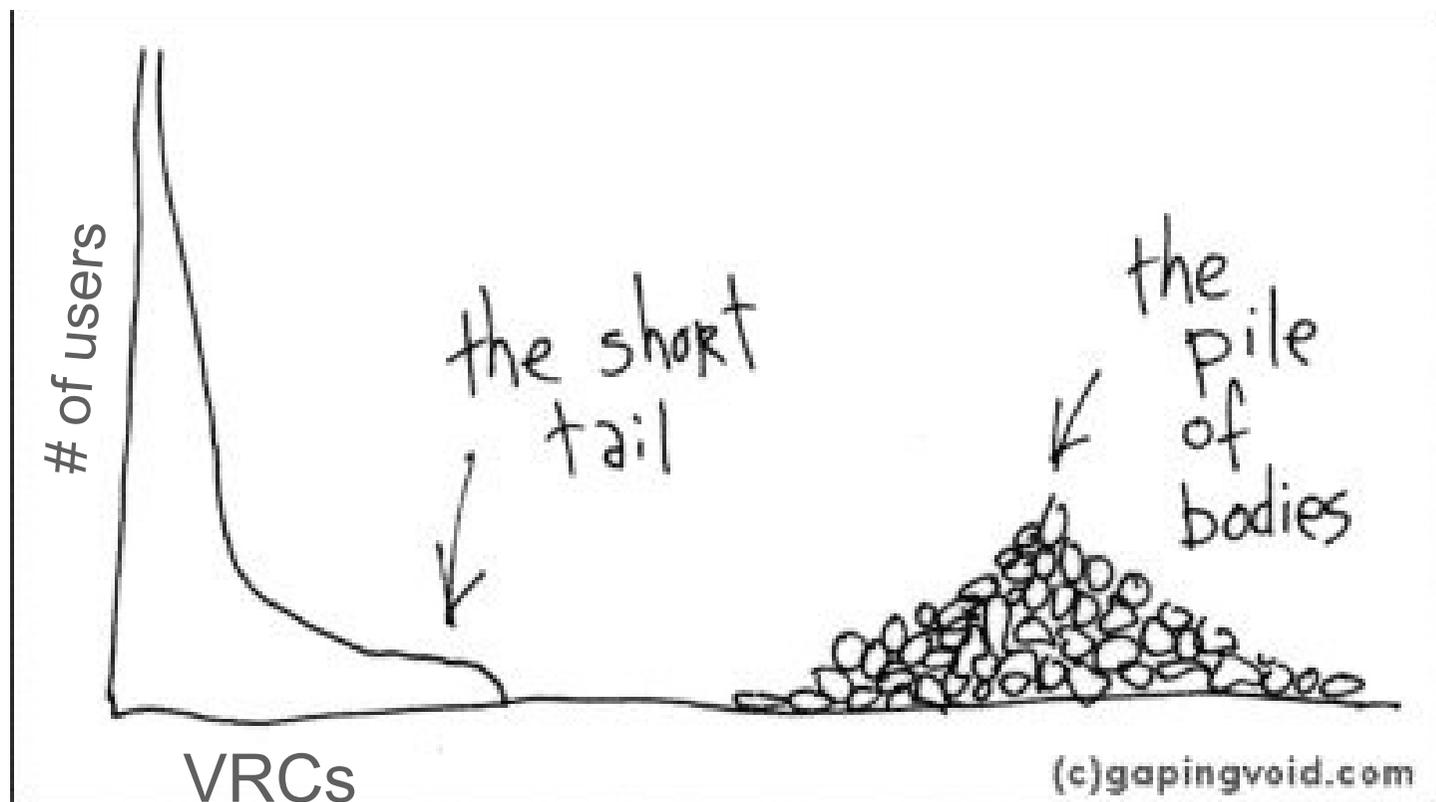
**L'esperienza dei Progetti DECIDE e INDICATE**

# I problemi da affrontare/1: **la troppa complessità**

- Grid offre calcolo e archiviazione “*on demand*”, ma è complessa e scarsamente user-friendly
- I ricercatori vogliono fare i ricercatori... Non diventare esperti di ICT
  - *In particolare, l'autenticazione attraverso certificati personali è visto come una vera e propria barriera d'accesso*



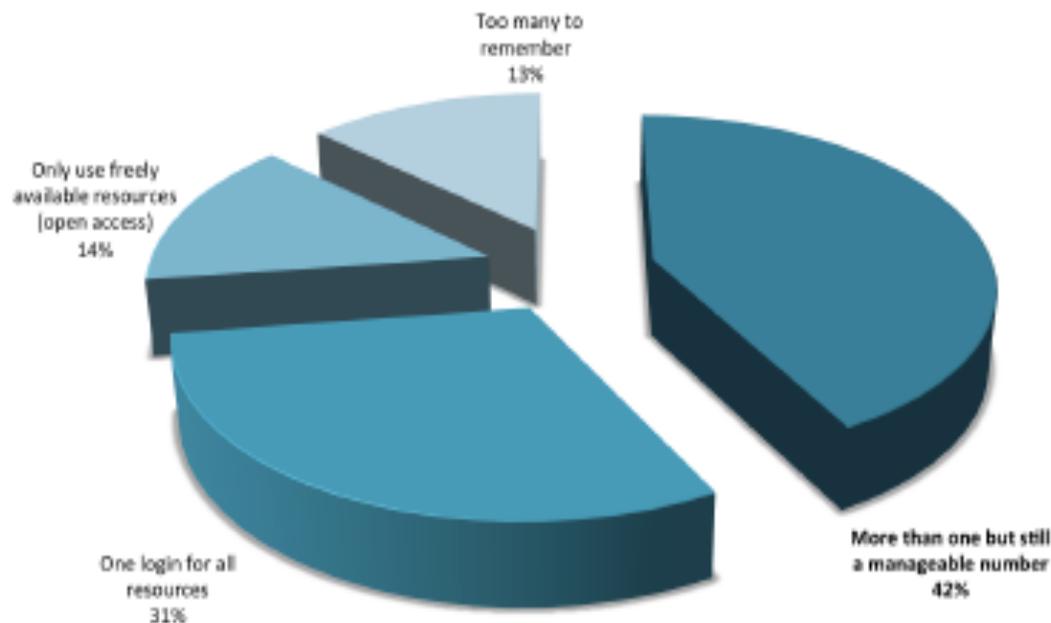
# I problemi da affrontare/1: **la troppa complessità**



La maggior parte degli utenti non fa parte di nessuna VRC  
*(e non ne sente la mancanza)*

## I problemi da affrontare/2: troppi metodi di autenticazione

- La maggior parte dei ricercatori usa più di un set di credenziali... *E di questi, quasi tutti ne farebbero volentieri a meno!*



FONTE: TERENA Study on “Advancing Technologies and Federating Communities”



# Le opportunità da sfruttare: l'avanzata delle Federazioni

## Le federazioni:

- rappresentano un'efficace risposta ad entrambi i problemi...
- Sono in rapida ascesa in Europa e non solo
- Permettono di conciliare la semplicità con la sicurezza, irrinunciabile per alcune comunità (es: medica)
- Sono una tecnologia condivisa a livello europeo e mondiale nel mondo della ricerca
- Aggiornamento in tempo reale: se un utente va via da un'organizzazione, non devo revocare certificati e permessi

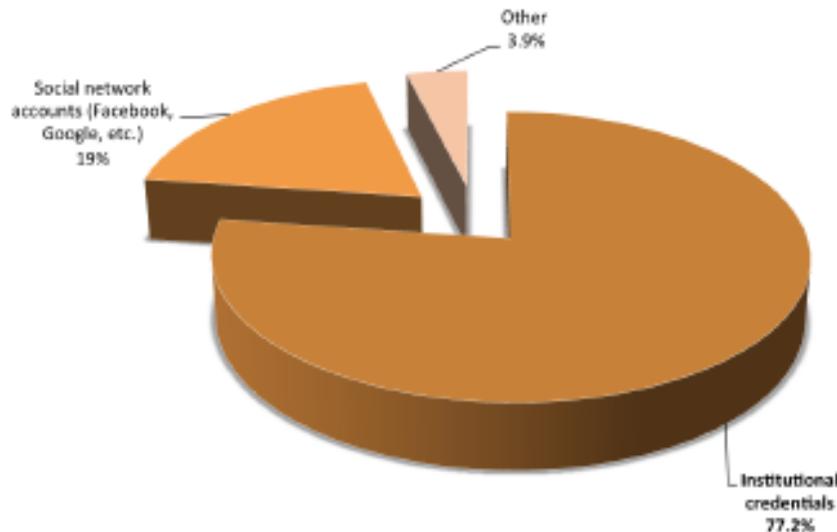
*... Quindi non si possono ignorare in un tool che promette di portare le e-infrastructures alla portata degli utenti*



# Non solo federazioni

- Un numero tutt'altro che insignificante di ricercatori usa le credenziali ottenute da un social network per accedere a informazioni scientifiche o legate a attività istituzionali:

*Perché ignorarli?*



- *E poi ci sono quelli per cui bisogna comunque creare le credenziali!*

FONTE: TERENA Study on “Advancing Technologies and Federating Communities”



# La filosofia dell'esperimento in una parola: **Convergenza**

- Mascherare la complessità e massimizzare la facilità di utilizzo per avvicinare le comunità a servizi complessi di tipo Grid/Cloud
  - *Non costringere l'utente a lavorare con un metodo scelto da noi, ma accettare tutti i mezzi scelti dall'utente!*

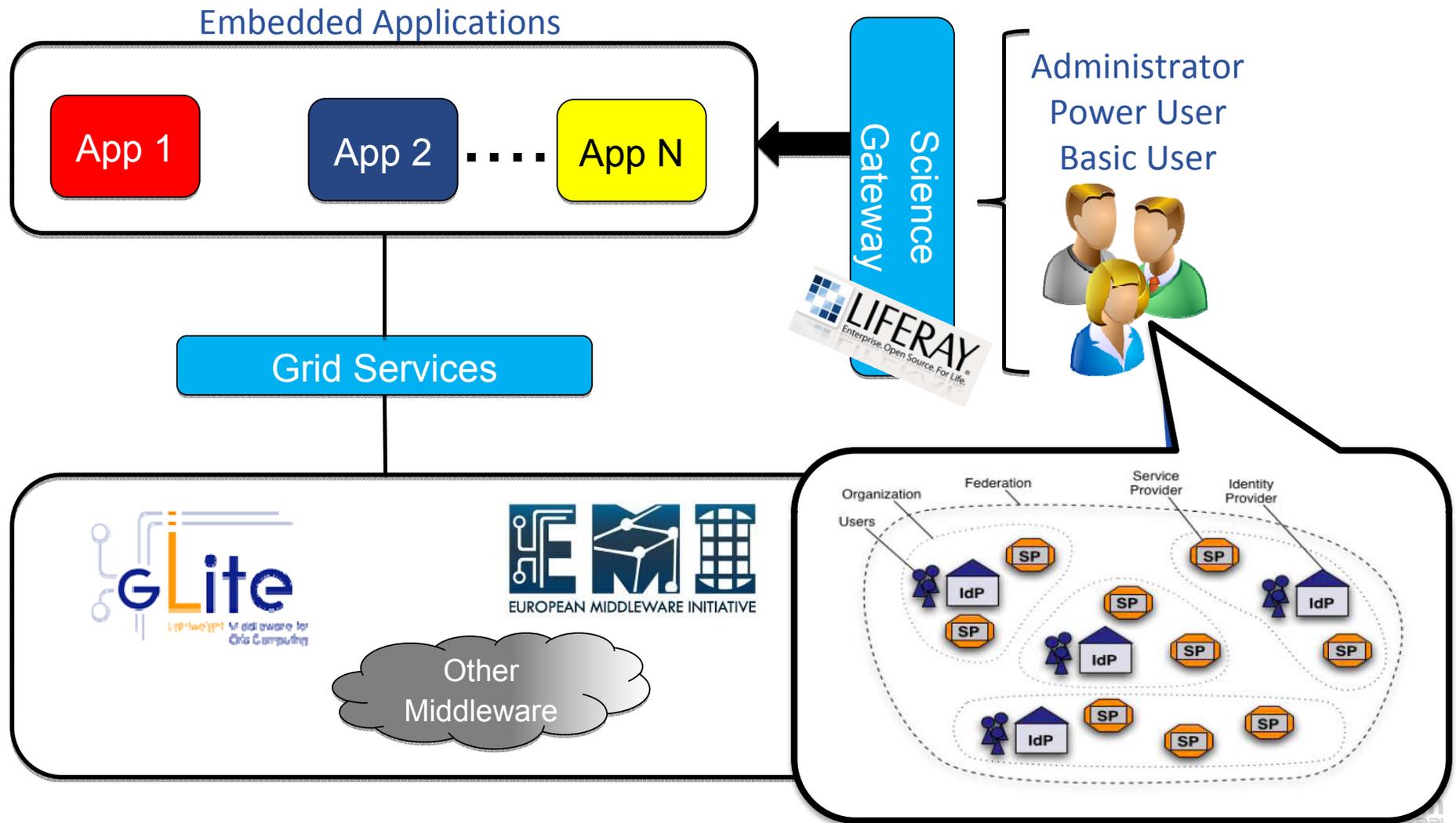


# Come: disaccoppiare Autenticazione e Autorizzazione

- Disaccoppiando le 2 fasi del processo...
  - L'utente si autentica con qualunque metodo a sua disposizione
  - Una volta autenticato l'utente, lo Science Gateway gli attribuisce dei permessi in base al suo profilo
  - *Quali metodi di autenticazione siano ammissibili per un certo Science Gateway diventa una questione di policy, che può essere definita a livello della singola comunità/progetto*



# Lo schema di riferimento



# Le raccomandazioni a livello europeo

<p>Enhance existing AA infrastructures to address the demands of research communities for accessing different types of services in a manageable and secure way.</p>	<p>AAA support for mobile access;</p> <p>Support for non-Web browser applications;</p> <p>Develop security token translation services to enable inter-operability of different AAs;</p> <p>Provide guest IdPs for users that cannot rely on an institutional IdP;</p> <p>Allow for effective resource usage accounting for distributed and heterogeneous environments;</p> <p>Enable the uptake and use of persistent identifiers within AAs;</p> <p>Support social network identities in combination with institutional identities to address specific use-cases for the SDI</p>	<p>National Identity Federations, eduGAIN, Research collaborations (i.e., big scientific projects)</p>	<p>Technical</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------	------------------

FONTE: TERENA Study on “Advancing Technologies and Federating Communities”



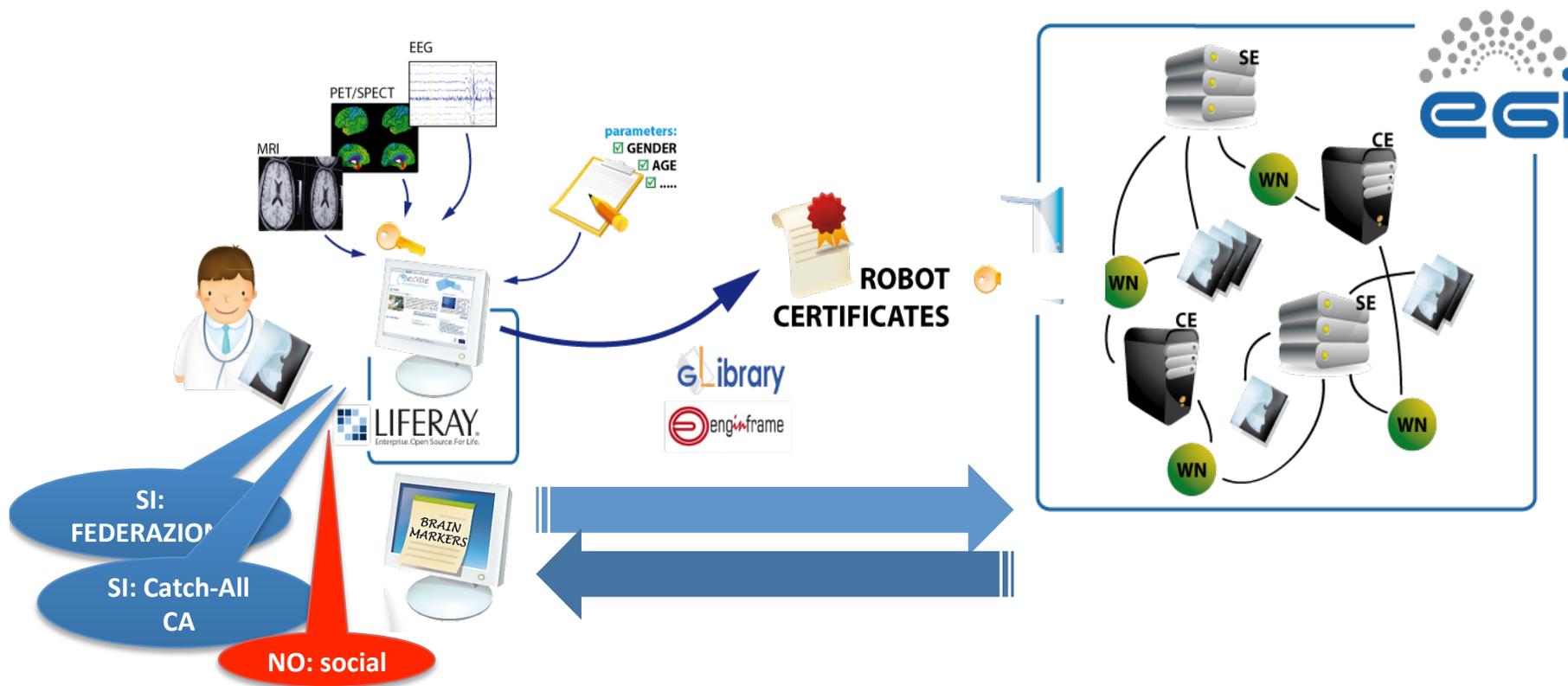
# E la loro implementazione..

- Con l'esperienza degli Science Gateway, il GARR è tra le prime NREN in Europa a implementare le raccomandazioni del TERENA AAA Study
  - Integrazione con Federazioni di Identità e EduGAIN
  - GrIDP <https://gridp.garr.it> (per utenti Grid)
  - IDPOPEN (formerly IDPCT) <https://idpopen.garr.it> (per utenti che abbisognano di nuove credenziali)
  - IdP Social <https://idpsocial.garr.it> (per l'integrazione delle identità "social")

*(operati da GARR, in collaborazione con INFN Catania)*



# L'esempio dello Science Gateway di DECIDE



- Disegnato per supportare diversi metodi d autenticazione (*senza certificati*)
  - Integrato con IDEM federazioni di identità
  - No social per alti requirement di sicurezza (ma può essere integrato)
- Basato su certificati “robot” gestiti dal sistema: niente certificati personali da gestire per l’utente
- Profili e livelli di autorizzazione multipli



# L'esempio dello Science Gateway di INDICATE

**Identity Federations' discovery service**

Select an Identity Provider

The service you are trying to reach requires that you get authenticated. Please, choose the Identity Provider you want to use and the Organisation you belong to.

Federation	Organisation
GARR-IDE	CASPUR
GridP	CILEA
All Sites	CINECA
	Consortium GARR sede di Firenze
	Fondazione IRCCS Policlinico San Matteo
	GARR FI idp2
	GARR FI idp215
	http://fed.amm.unibs.it/fed/idp
	https://idp-shib.unisanno.it/idp/shibboleth
	https://idp.unipi.it/idp/shibboleth

Select Remember for session

In case of problem

**Do not bookmark this page!**

After login you will be redirected to the web page containing the service of the portal you wanted to use.

 **Shibboleth.**

**Shibboleth Identity Provider Login to Service Provider https://indicate-gw.conorzio-cometa.it/shibboleth**

Existing Session: false  
 Requested Authentication Methods: []  
 Attempting Authentication Method: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport  
 Is Forced Authentication: false

Username: test1  
 Password: \*\*\*\*\*  
 Login

**Identity Provider Catania «catch-all» Identity Provider**

**Login Page**

In order to use this service of the portal https://indicate-gw.conorzio-cometa.it, please enter below the credentials provided to you by the Identity Provider:

User: barbera  
 Password: \*\*\*\*\*  
 Login

**Lost/forgotten Credentials**

If you have lost or forgotten your credentials, please send an email to [credentials-admin\\_AT\\_ct.infn.it](mailto:credentials-admin_AT_ct.infn.it)

**Do not bookmark this page!**

After login you will be redirected to the web page containing the service of the portal you wanted to use.



- Gateway di accesso agli archivi culturali
- utilizza il *single sign-on* offerto dalle Federazioni
- Nel pilota, l'eCulture science gateway di INDICATE è stato configurato come *Service Provider* di IDEM e CARSI (carsi.edu.cn).



# Concludendo...

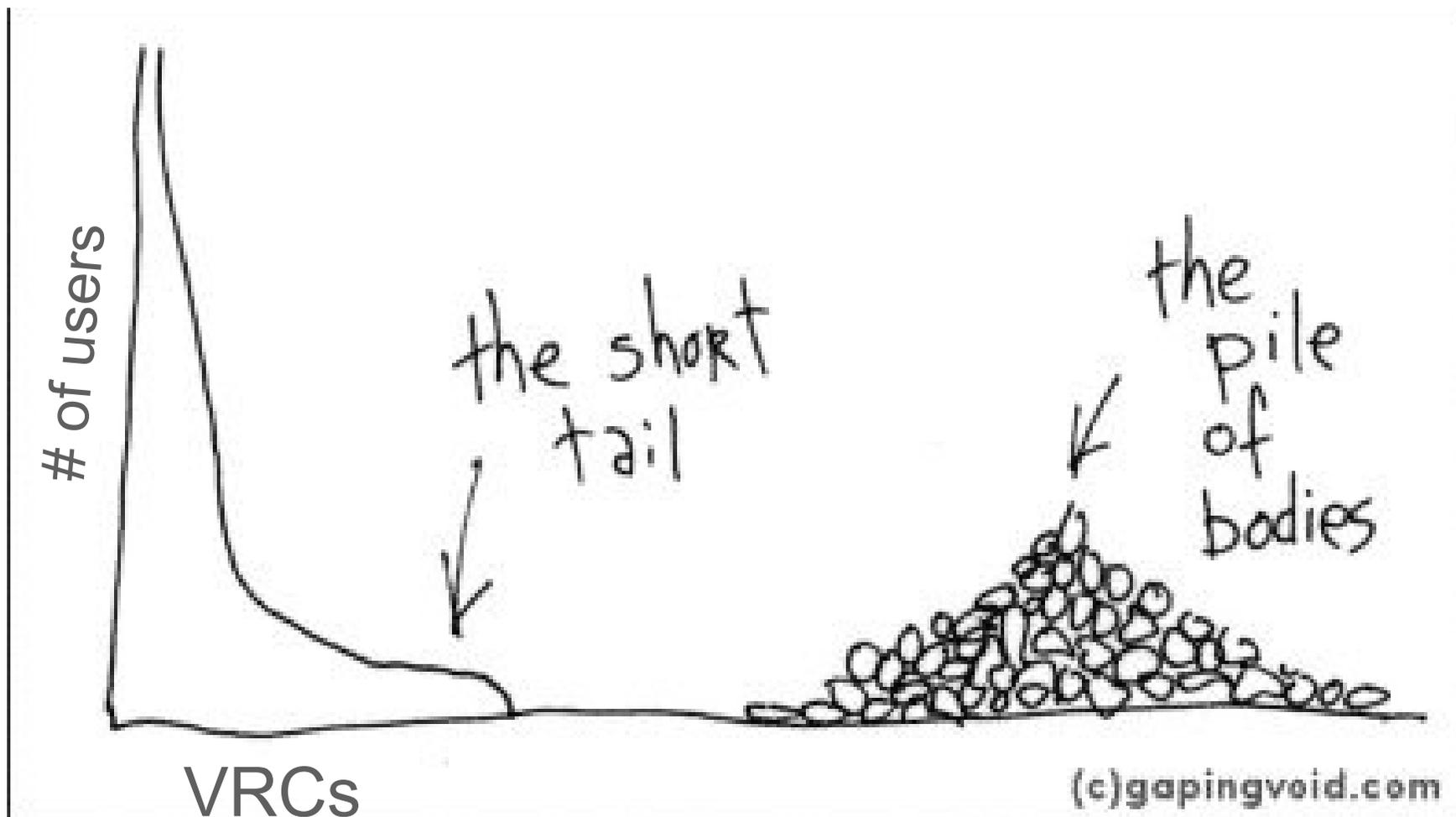
- L'integrazione tra Federazioni e SG è una realtà
- Passo importante verso l'adozione delle infrastrutture digitali da parte di un numero sempre maggiore di utenti non esperti
  - offrendo loro risorse (calcolo, storage, applicativi...) che gli erano precluse
  - rendendo accessibili risorse di grande valore a tantissimi soggetti, dal ricercatore fino allo studente  
(biblioteche digitali, repository culturali, grandi banche dati biomediche....)
- Preferibile ad altri metodi per sicurezza e aggiornamento
- Il feedback degli utenti è molto positivo e rappresenta un aspetto di spinta dal basso ad aderire

# Concludendo/2

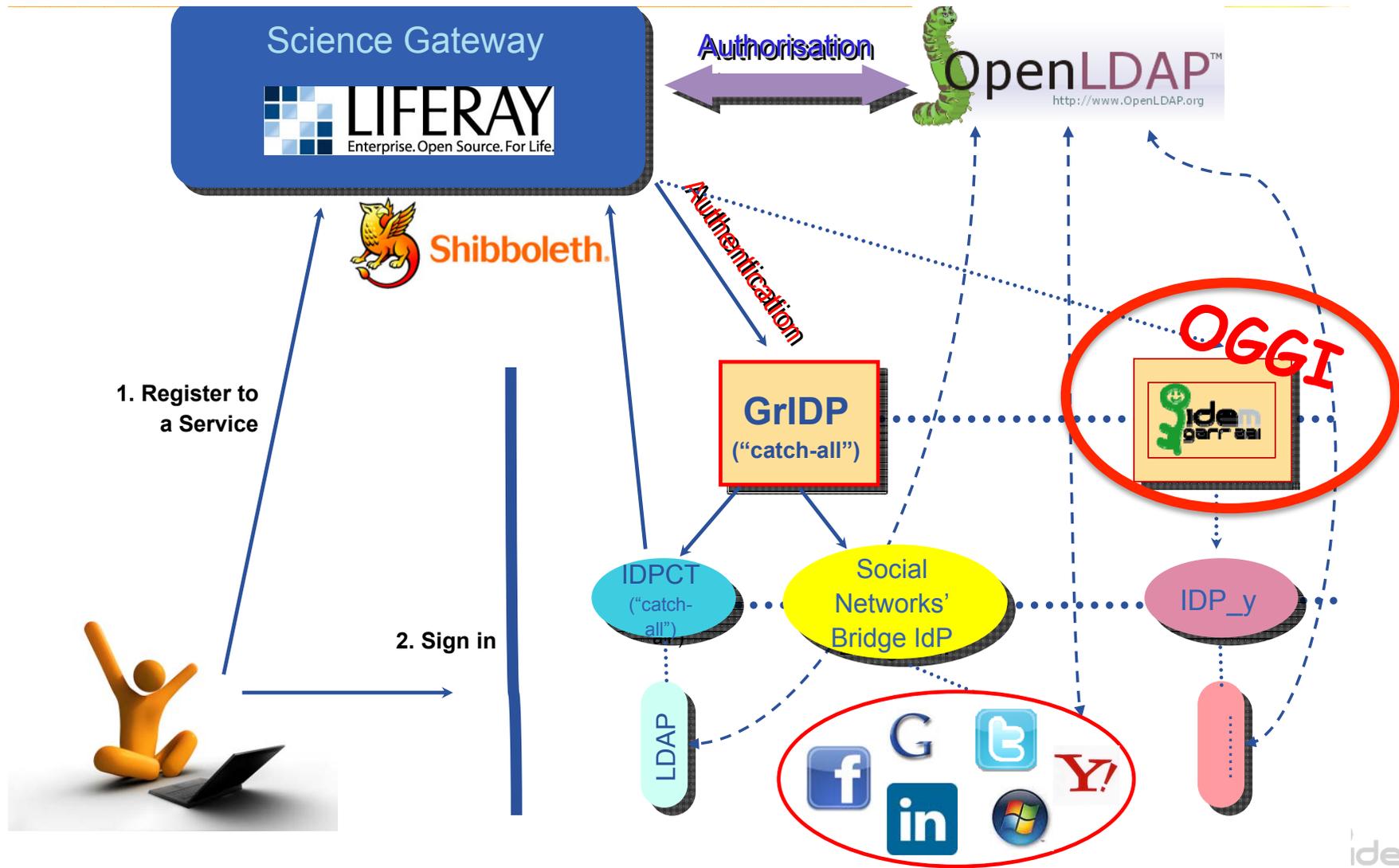
Unico limite per questo scenario:

- Ci sono ancora molte comunità al di fuori delle federazioni
- Fare in modo che l'accesso non sia percepito come una barriera rendendolo semplice
  - IdP in the Cloud è un passo in questa direzione
- Senza semplificare, il rischio è di ricadere nell'errore delle VRC!

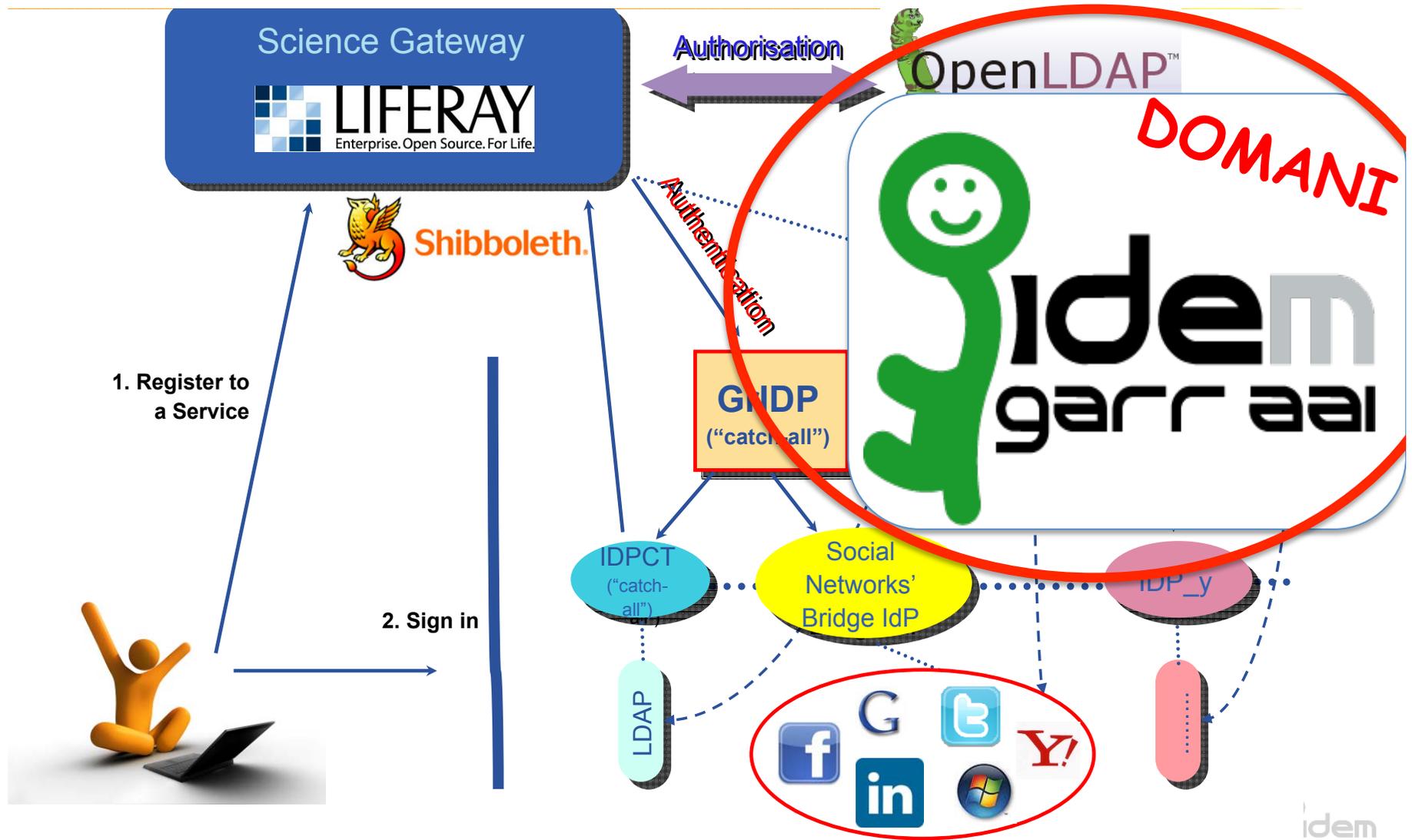
# Concludendo/2



# Un obiettivo per il futuro:



# Un obiettivo per il futuro:



The image features a hypnotic, swirling pattern of concentric circles in vibrant red and purple. The circles are arranged in a way that creates a strong sense of depth and movement, drawing the viewer's eye towards the center. Overlaid on this pattern is the text "That's all Folks!" written in a classic, white cursive font with a subtle drop shadow, making it stand out against the colorful background.

*That's all Folks!*