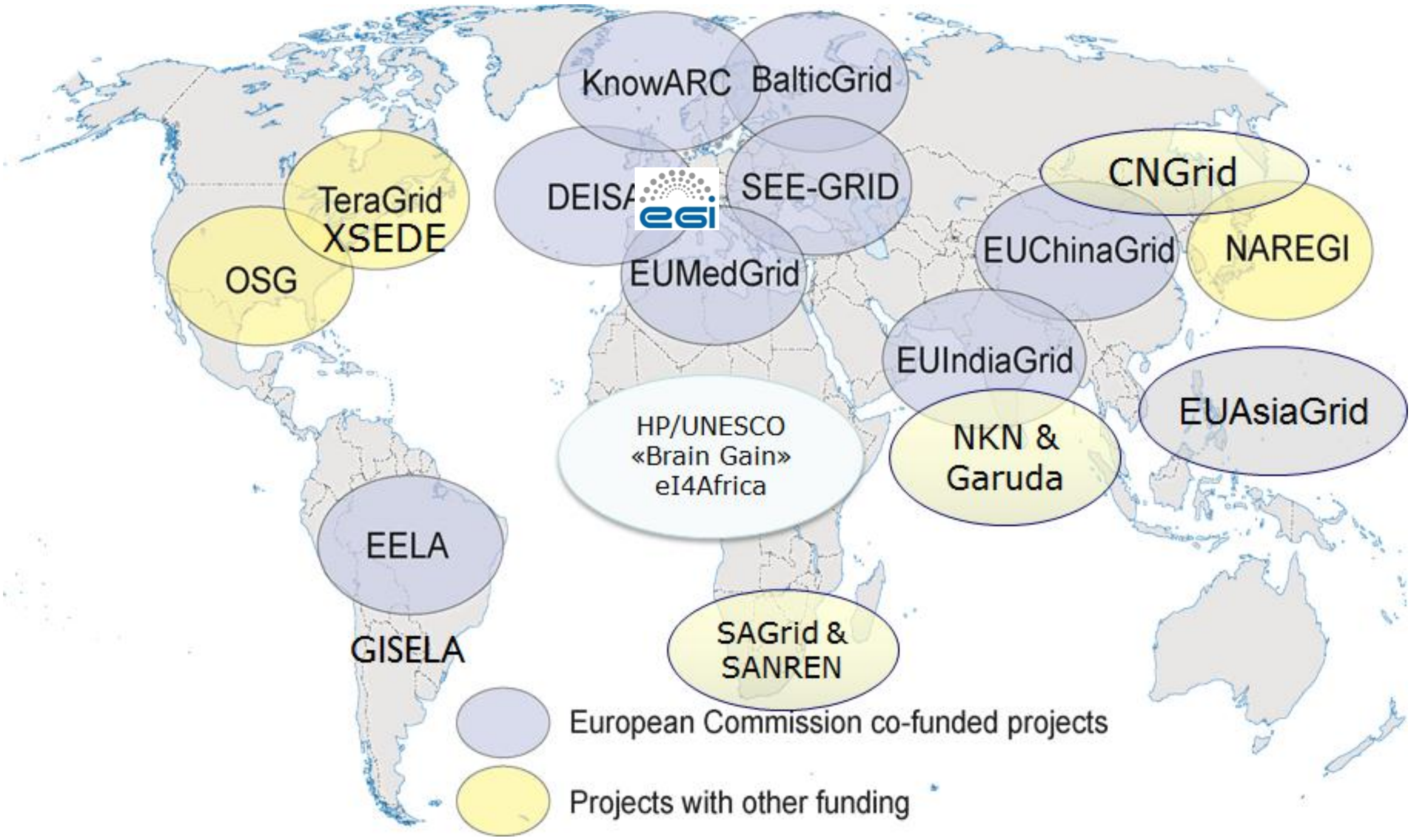
Federated access to e-Infrastructures worldwide

Marco Fargetta, INFN Catania - Italy

(marco.fargetta@ct.infn.it)

VAMP Workshop 2013 – Helsinki, 30/9-1/10/2013

DCIs developed in the last decade



Evolution

- **Research organisations are moving to cloud computing**
  - Internal services and research applications
- **Many different cloud models**
  - Public vs Private vs Commercial
  - IaaS, PaaS, SaaS
- **Grid paradigm still adopted by many projects**
  - Grid and cloud will co-exist for a while
  - Many mixed approach are under investigation and testing

e-Infrastructures problems

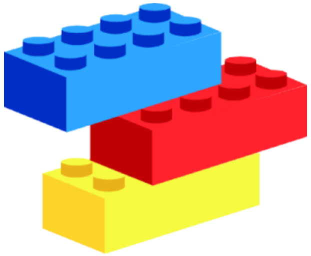
- **Different authentication/authorisation**
  - Username/password, X509, others
- **Different tools to interact with**
  - GUI, CLI, API, Web Apps, Web Services, etc…
- **Different middleware and workflows to execute applications**
- **Very little standard adoption**
  - Lack of interoperability
- **Difficult for users to move from a system to another**

Science Gateways

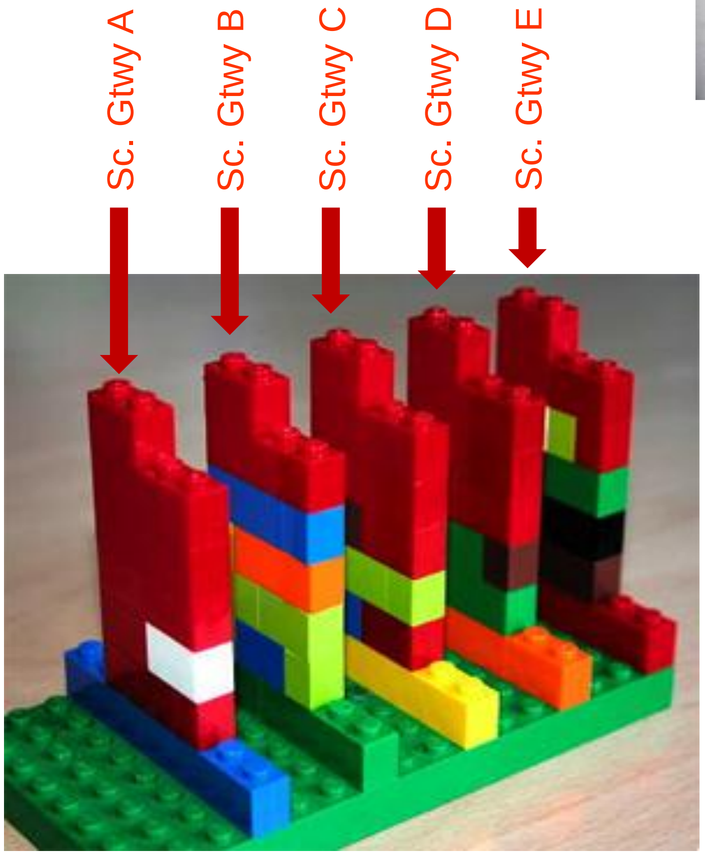
“A Science Gateway is a community-developed set of tools, applications, and data that is integrated via a portal or a suite of applications, usually in a graphical user interface, that is further customized to meet the needs of a specific community.”

Teragrid/XSEDE

Primary requirement: building Science Gateways should be like playing with Lego bricks



- Standards
- Simplicity
- Easiness of use
- Re-usability



Sc. Gtwy A

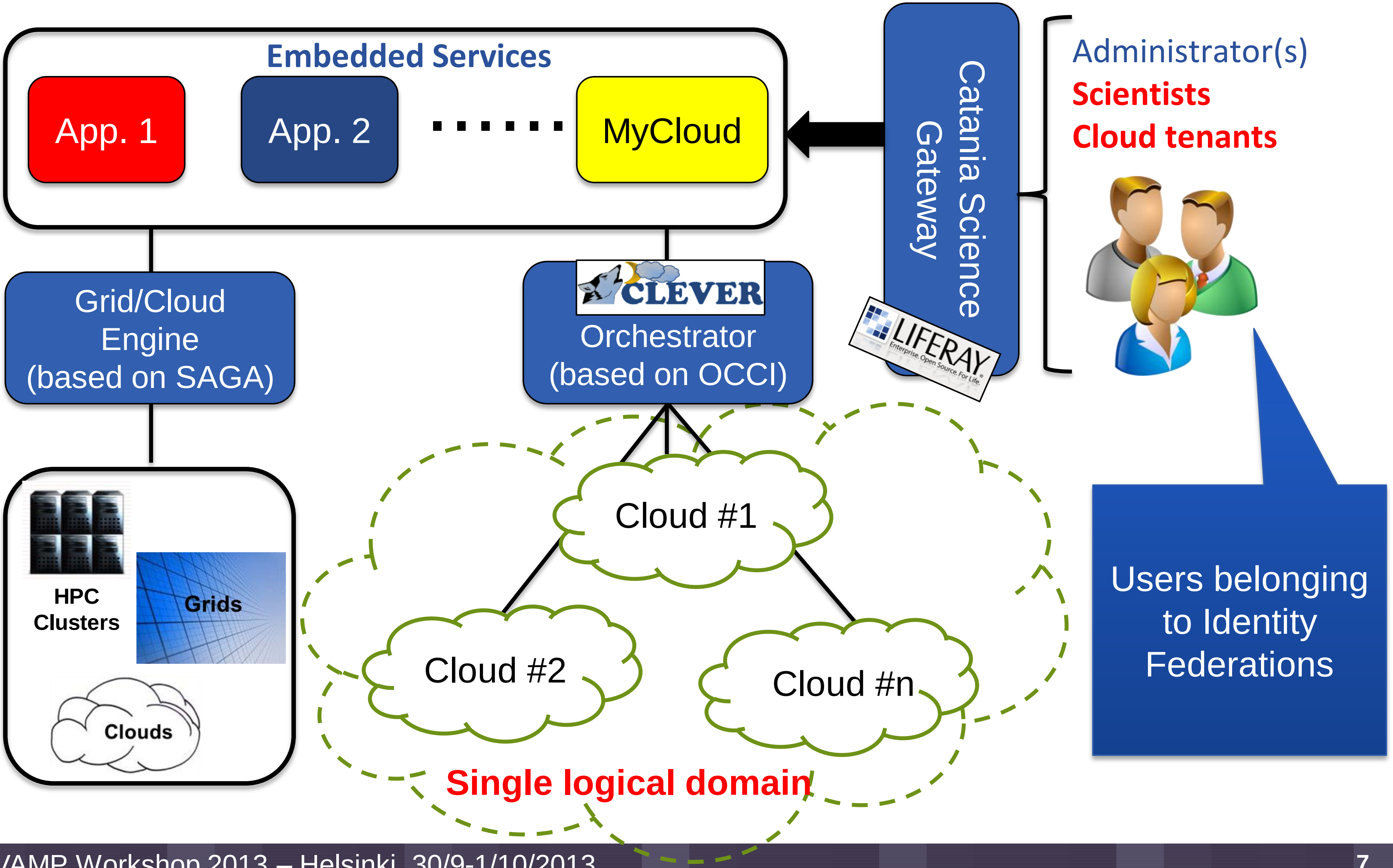
Sc. Gtwy B

Sc. Gtwy C

Sc. Gtwy D

Sc. Gtwy E

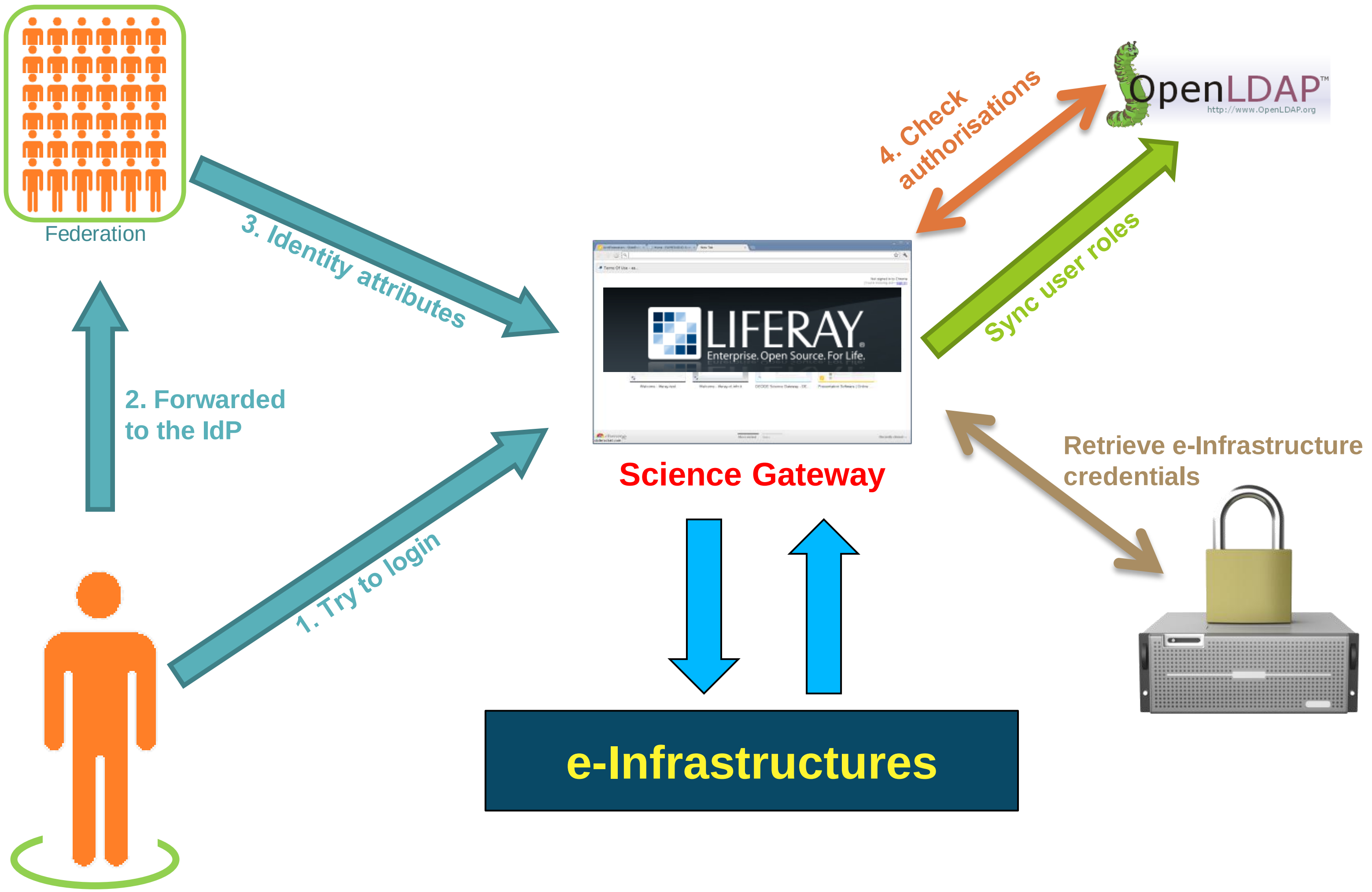
Catania Science Gateway Framework architecture



Unified authentication system

- **Users have to use only one account for all the systems**
  - The account is generally provided by the home institution
  - SAML2.0 used
- **Authentication to e-Infrastructure is performed by the Science Gateway**
  - e-Infrastructures do not distinguish Science Gateway users
  - User tracking DB implemented for accounting and auditing purposes, compliant with EGI policies

AuthN/AuthZ Schema



Federation

1. Try to login

2. Forwarded to the IdP

3. Identity attributes

4. Check authorisations

Sync user roles

Science Gateway

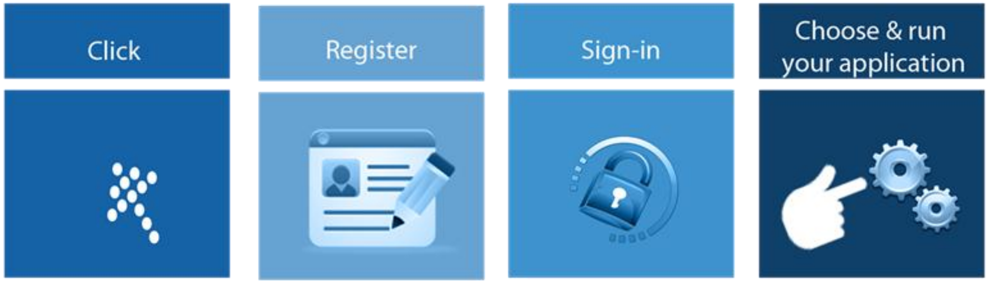
Retrieve e-Infrastructure credentials

e-Infrastructures

Science Gateways deployed

12 SGs in production and others in development

VRCs supported either by region or discipline



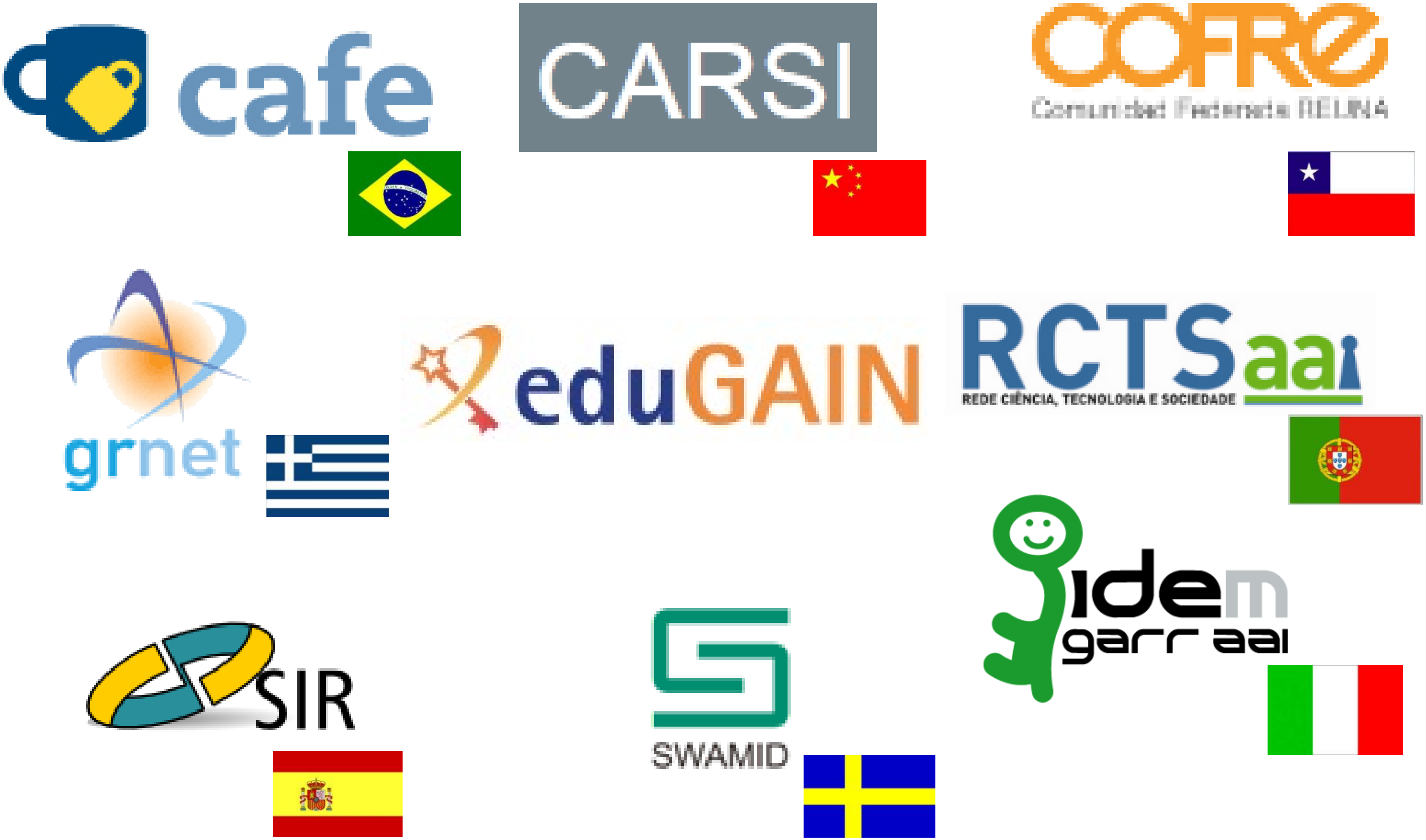
Very easy and intuitive access procedure

User-driven development

Surveys to propose applications are available in Italian and other languages

- Africa Grid
- agINFRA
- CHAIN-REDS
- COGITO-MED
- DCH-RP e-Culture
- DECIDE
- EarthServer
- EUMEDGRID
- GARR
- GISELA
- IGI
- KLIOS

Official Identity (Inter-)Federations currently supported by Catania Science Gateways



The TERENA AAA Study (Objectives)

https://confluence.terena.org/display/aaastudy/AAA+Study+Home+Page

European Commission

Advancing Technologies and Federating Communities

A Study
on Authentication
and Authorisation Platforms
For Scientific Resources
in Europe

FINAL REPORT
A study prepared for the European Commission
DG Communications Networks, Content & Technology

Digital Agenda for Europe

The goal has been broken down into two objectives:

1. **A collection of users' access requirements coming from different communities;**
2. **A gap analysis of the existing AAIs used in the realm of research and education, the use-cases they support and the associated challenges.**

The TERENA AAA Study (Findings)

Researchers primarily use their institutional credentials for authentication (Figure 2.3), although a not insignificant number (19%), use their social network account credentials to access scientific information.

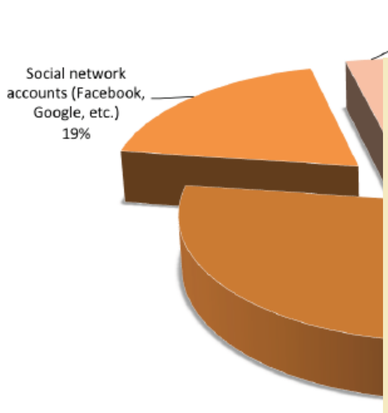


Figure 2.3: Credentials used by researchers

Nearly half of researchers use more than one credential, but a large majority would prefer to access all resources using their institutional credentials.

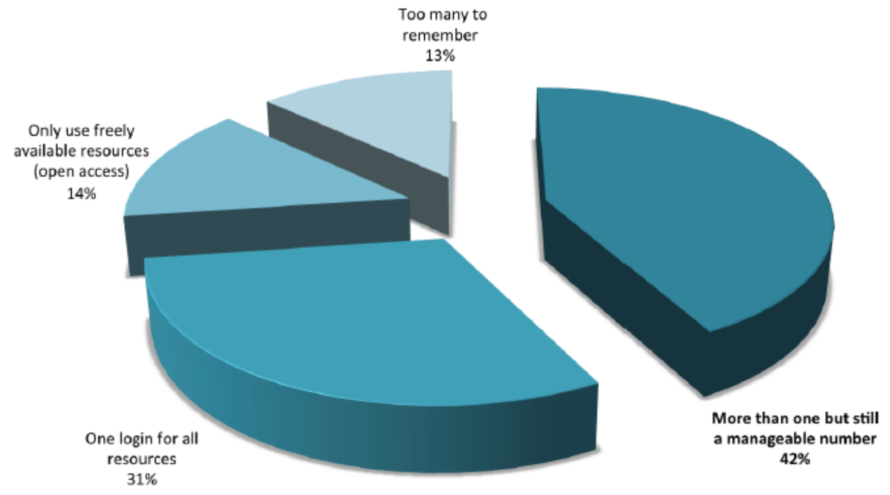
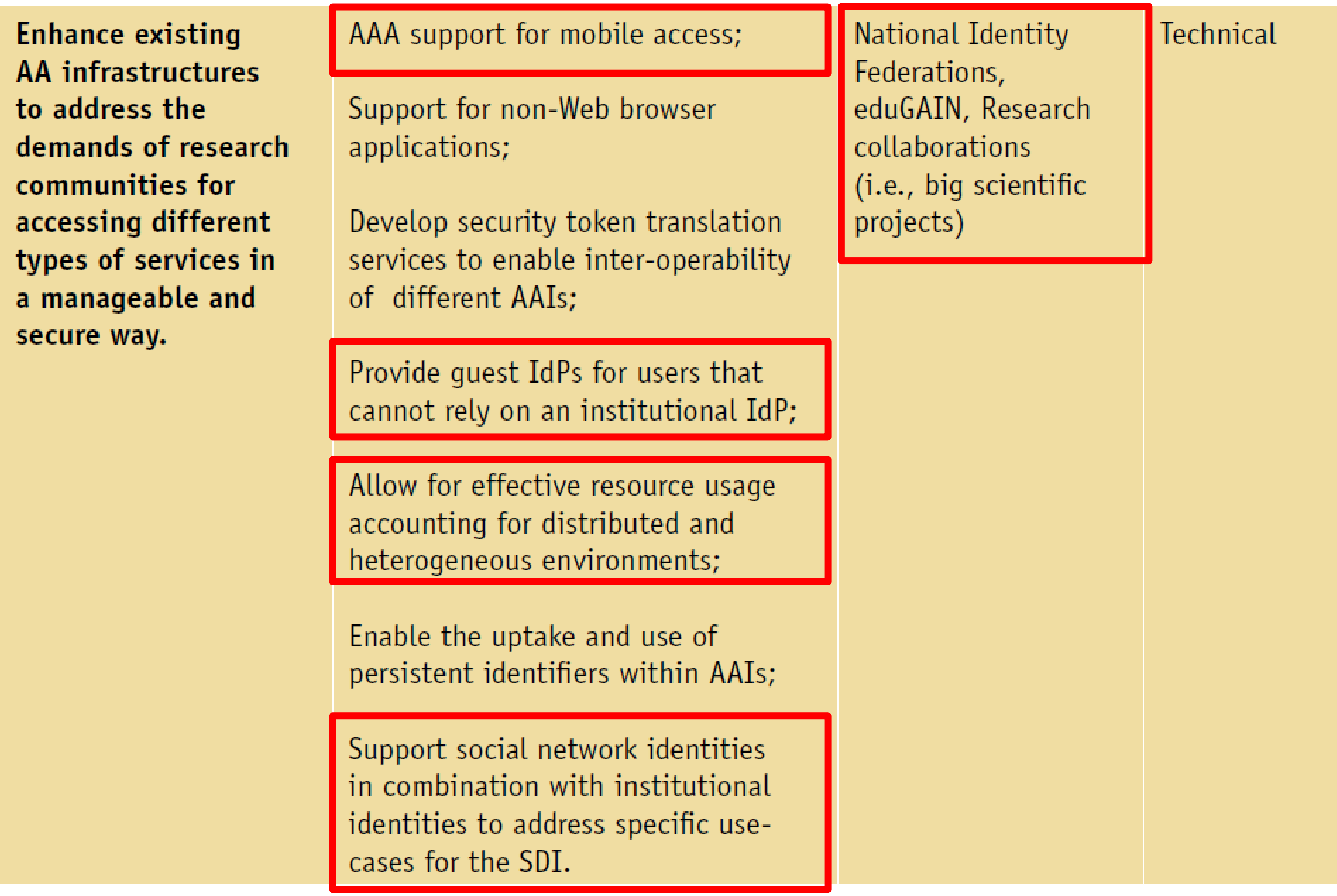


Figure 2.4: Number of credentials used by researchers

The TERENA AAA Study (Recommendations)



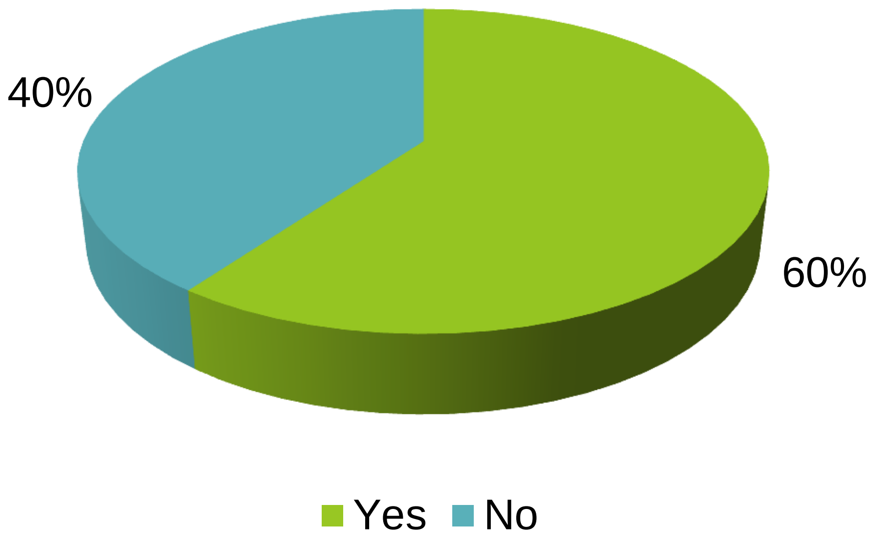
Recommendation	Action Required	Main Stakeholder(s)	Area
Enhance existing AA infrastructures to address the demands of research communities for accessing different types of services in a manageable and secure way.	AAA support for mobile access;	National Identity Federations, eduGAIN, Research collaborations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

DCH-RP AAI Survey
(www.dch-rp.eu)

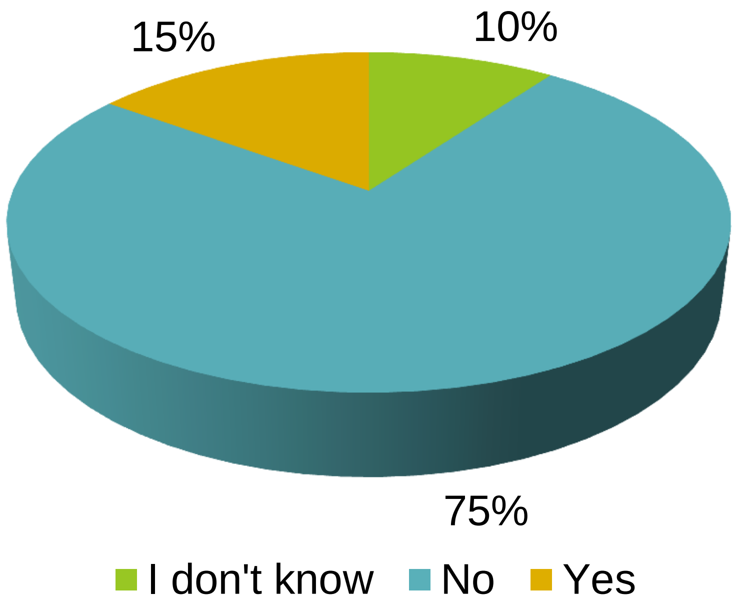
- **“Digital Cultural Heritage Roadmap for Preservation” (*DCH-RP*) is a coordination action supported by the European Commission under the e-Infrastructure Capacities Programme of Seventh Framework Programme for Research (FP7)**
- **A survey about the AAI performed both within and outside the project community**
  - Mainly research and cultural organisations
  - 20 organisations already filled the survey
  - http://dch-rp.eu/index.php?en/71/news-archive/6/dch-rp-questionnaire

DCH-RP AAI Survey
(Current findings)

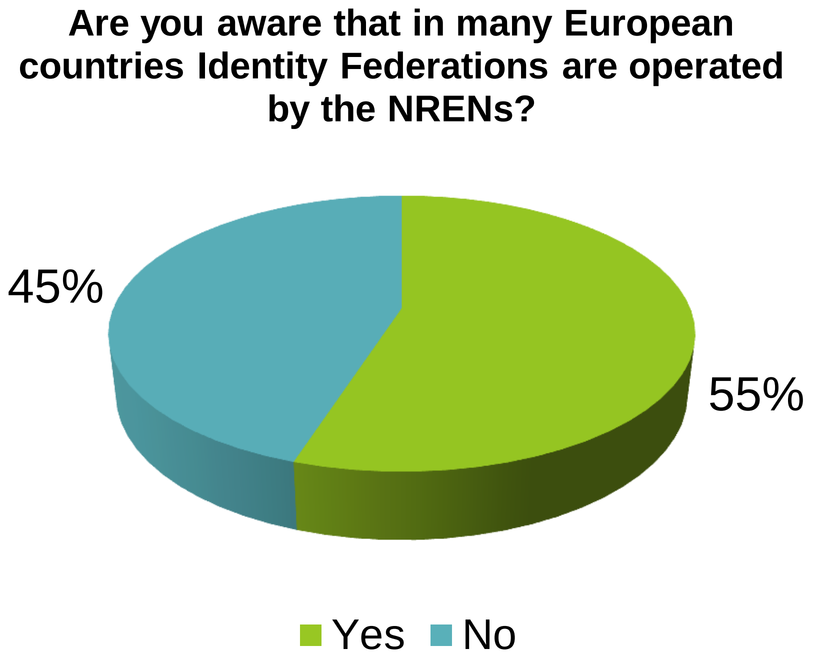
Are you aware of federated access or of Identity Federations?

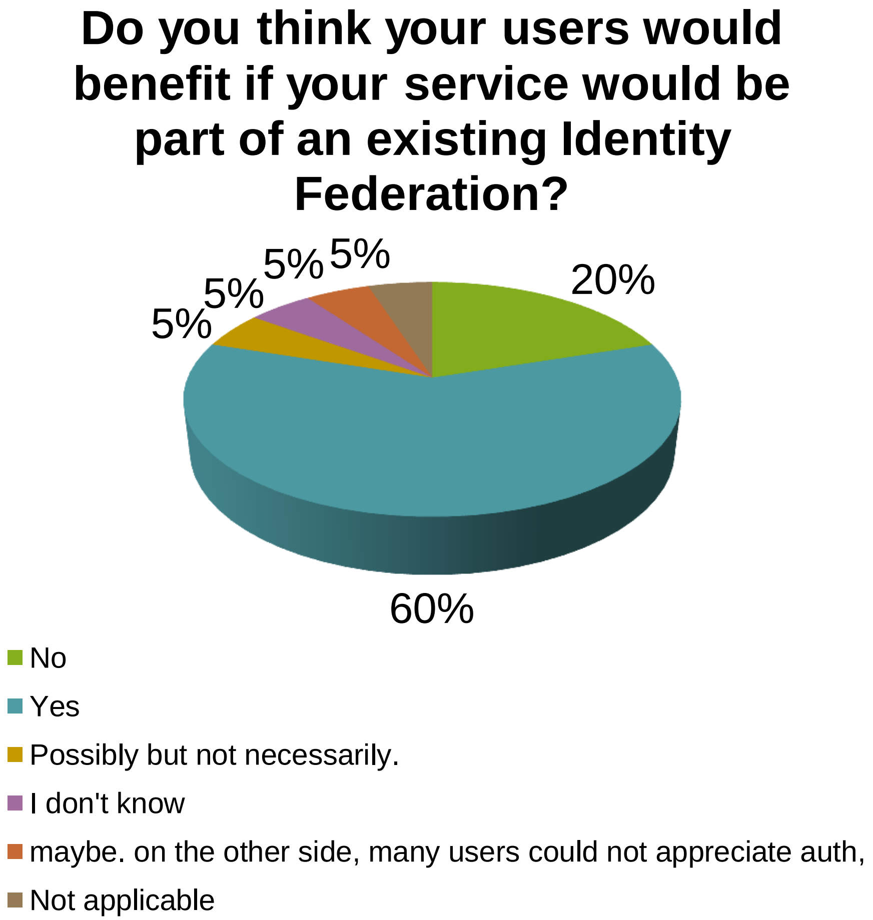


Is your institution part of a national Identity Federation?



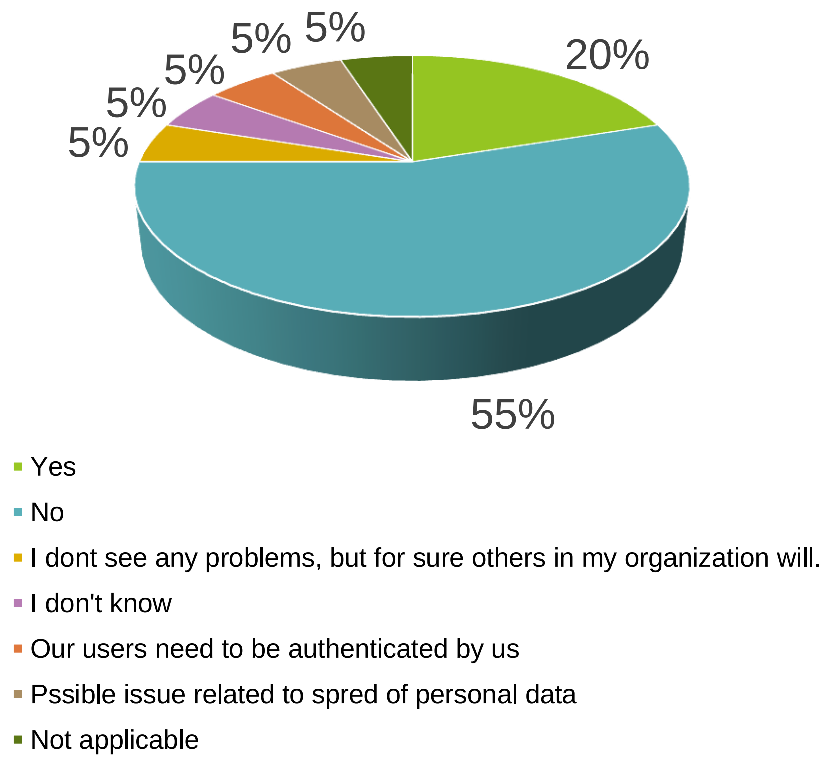
DCH-RP AAI Survey
(Current findings)



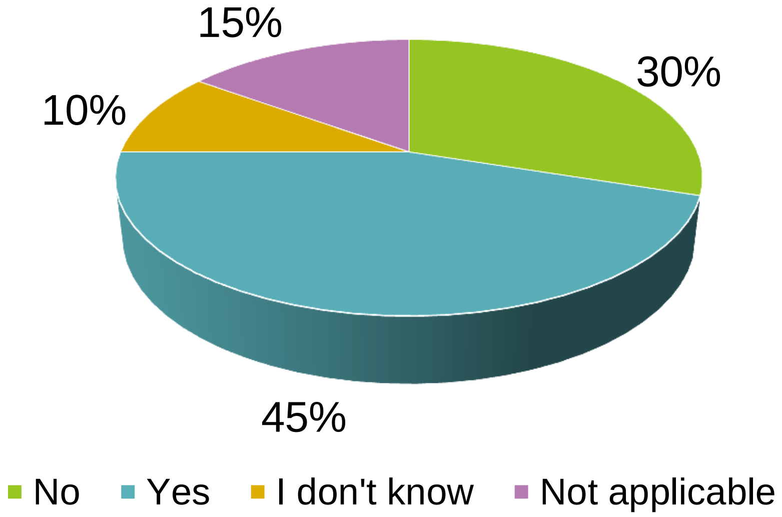


DCH-RP AAI Survey
(Current findings)

Do you see any problems if users, in order to access to your service, are authenticated by a "catch-all" Identity Provider?

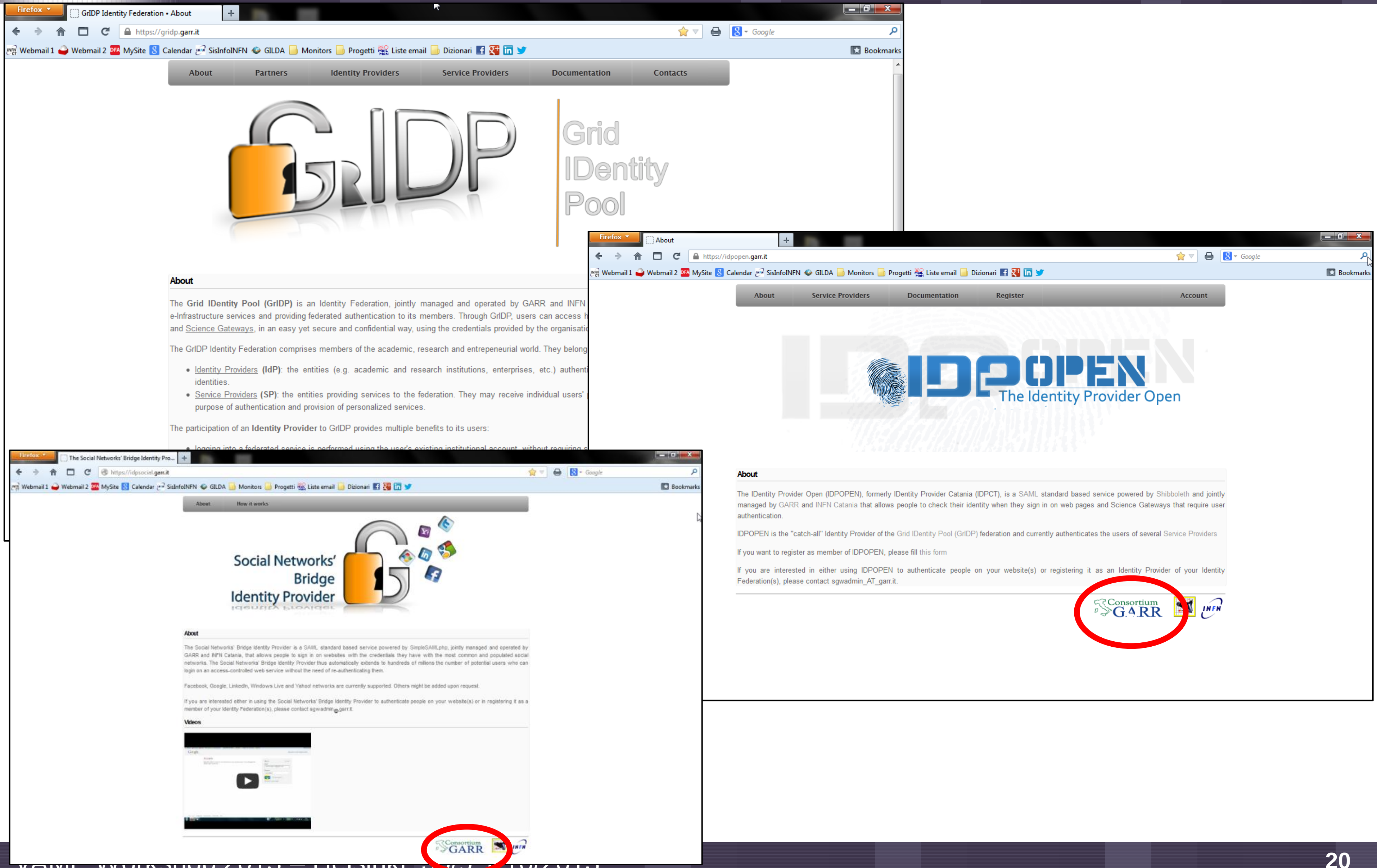


Would you like to get support to create an Identity Provider to manage users accounts for your organization?



The GrIDP "catch-all" federation

(http://gridp.garr.it)



About

The **Grid IDentity Pool (GrIDP)** is an Identity Federation, jointly managed and operated by GARR and INFN
e-Infrastructure services and providing federated authentication to its members. Through GrIDP, users can access h
and Science Gateways, in an easy yet secure and confidential way, using the credentials provided by the organisatic

The GrIDP Identity Federation comprises members of the academic, research and entrepeneurial world. They belong

- Identity Providers **(IdP)**: the entities (e.g. academic and research institutions, enterprises, etc.) authenti identities.
- Service Providers **(SP)**: the entities providing services to the federation. They may receive individual users' purpose of authentication and provision of personalized services.

The participation of an **Identity Provider** to GrIDP provides multiple benefits to its users:

- logging into a federated service is performed using the user's existing institutional account, without requiring s

About

The IDentity Provider Open (IDPOPEN), formerly IDentity Provider Catania (IDPCT), is a SAML standard based service powered by Shibboleth and jointly managed by GARR and INFN Catania that allows people to check their identity when they sign in on web pages and Science Gateways that require user authentication.

IDPOPEN is the "catch-all" Identity Provider of the Grid IDentity Pool (GrIDP) federation and currently authenticates the users of several Service Providers

If you want to register as member of IDPOPEN, please fill this form

If you are interested in either using IDPOPEN to authenticate people on your website(s) or registering it as an Identity Provider of your Identity Federation(s), please contact sgwadmin_AT_garr.it.

Consortium GARR
INFN
Firefox
The Social Networks' Bridge Identity Pro...
https://idpsocial.garr.it
About
How it works
Social Networks' Bridge Identity Provider

About

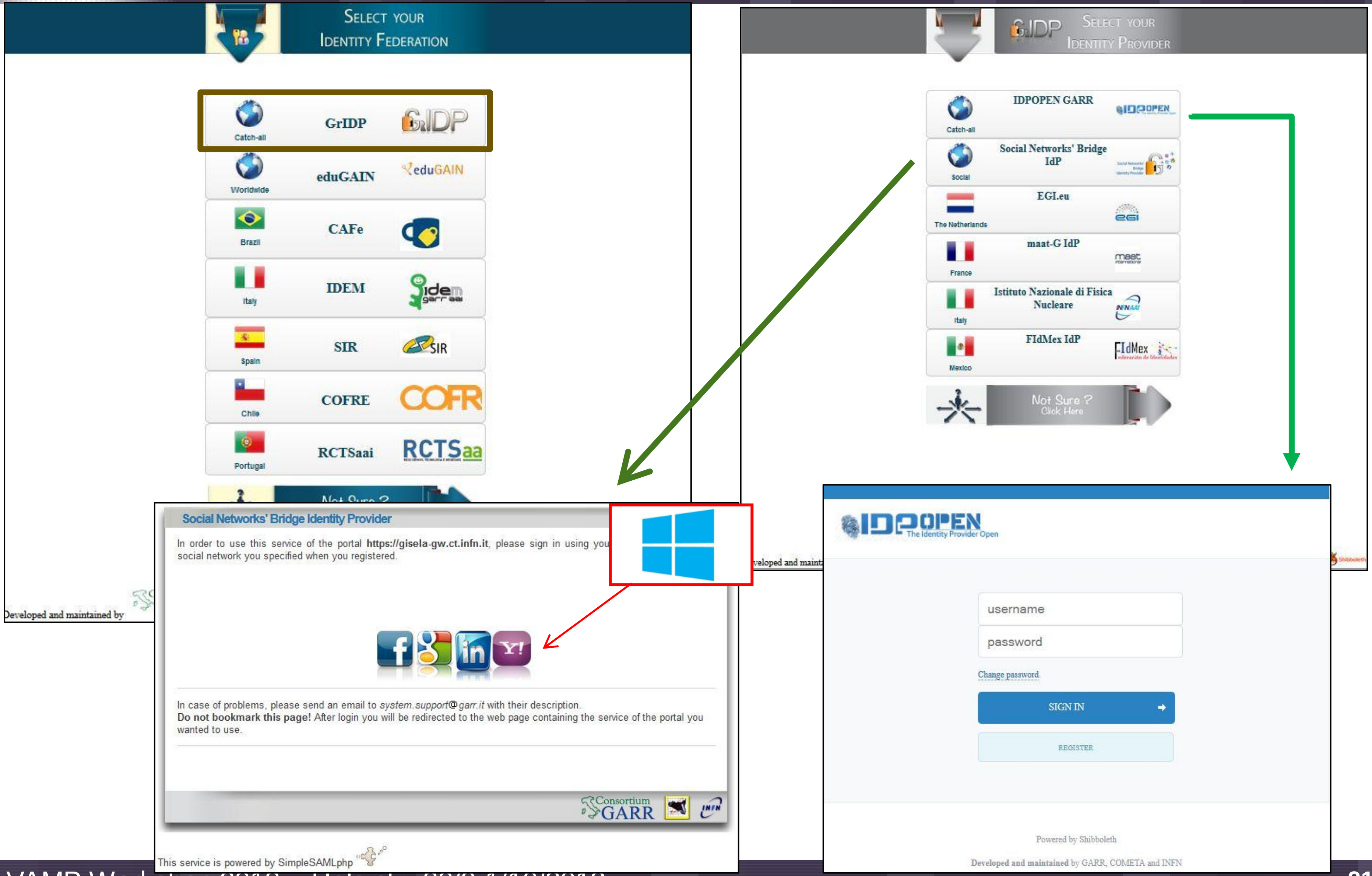
The Social Networks' Bridge Identity Provider is a SAML standard based service powered by SimpleSAMLphp, jointly managed and operated by GARR and INFN Catania, that allows people to sign in on websites with the credentials they have with the most common and populated social networks. The Social Networks' Bridge Identity Provider thus automatically extends to hundreds of millions the number of potential users who can login on an access-controlled web service without the need of re-authenticating them.

Facebook, Google, LinkedIn, Windows Live and Yahoo! networks are currently supported. Others might be added upon request.

If you are interested either in using the Social Networks' Bridge Identity Provider to authenticate people on your website(s) or in registering it as a member of your Identity Federation(s), please contact sgwadmin@garr.it.

Videos

The Open and Social IdP's



Select your Identity Federation

Catch-all	GrIDP	GrIDP
Worldwide	eduGAIN	eduGAIN
Brazil	CAFe	
Italy	IDEM	idem garr aai
Spain	SIR	SIR
Chile	COFRE	COFRE
Portugal	RCTSaai	RCTSaai

Not Sure ?

Developed and maintained by

GrIDP Select your Identity Provider

Catch-all	IDPOPEN GARR	IDPOPEN
Social	Social Networks' Bridge IdP	Social Network Bridge Identity Provider
The Netherlands	EGI.eu	egi
France	maat-G IdP	maat
Italy	Istituto Nazionale di Fisica Nucleare	INFN AAI
Mexico	FIdMex IdP	FIdMex Federación de Identidades

Not Sure ? Click Here

Developed and maint

Social Networks' Bridge Identity Provider

In order to use this service of the portal **https://gisela-gw.ct.infn.it**, please sign in using you social network you specified when you registered.

In case of problems, please send an email to *system.support@garr.it* with their description.
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.

Consortium GARR

This service is powered by SimpleSAMLphp

IDPOPEN The Identity Provider Open

username

password

Change password

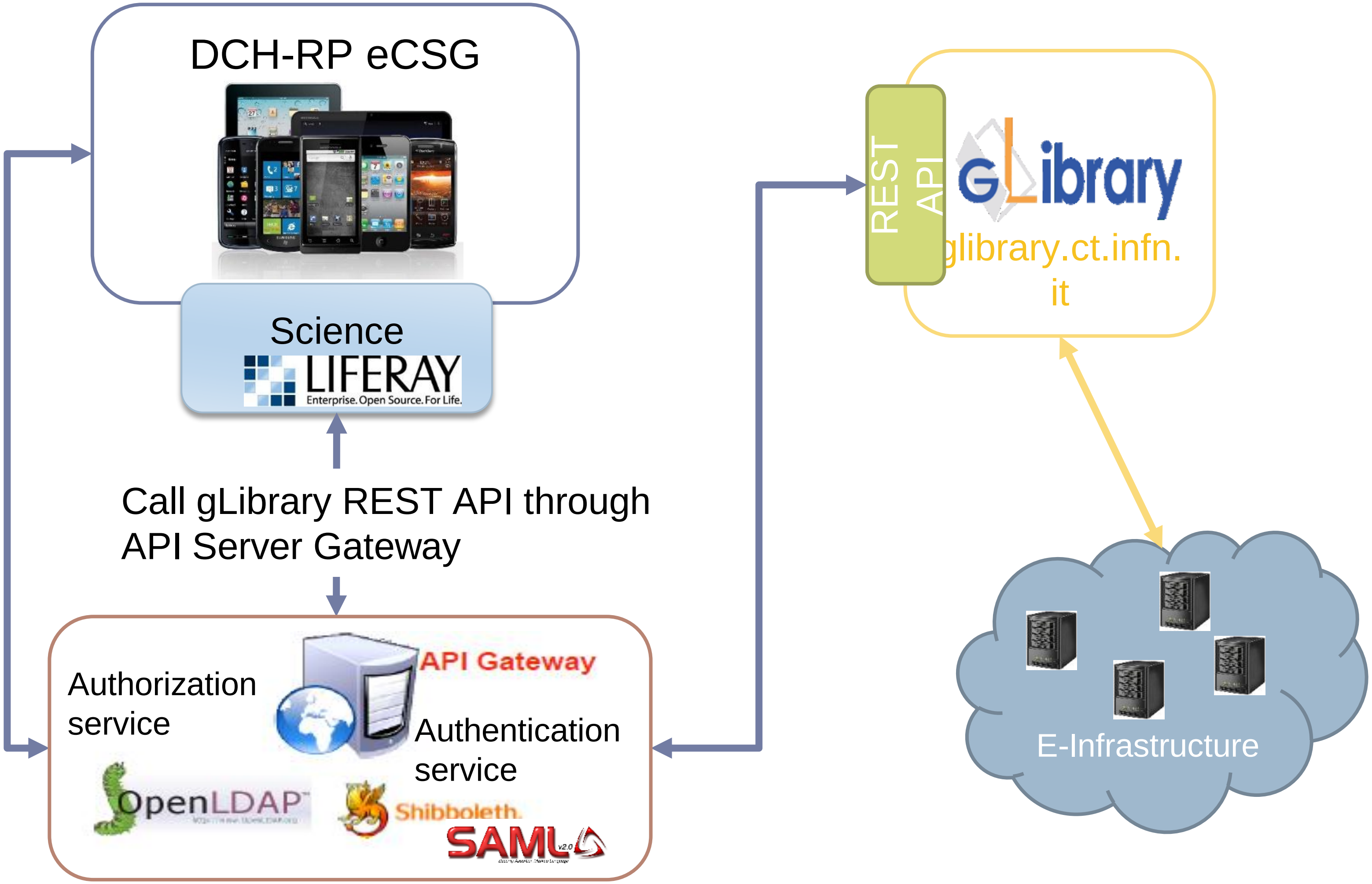
SIGN IN

REGISTER

Powered by Shibboleth

Developed and maintained by GARR, COMETA and INFN

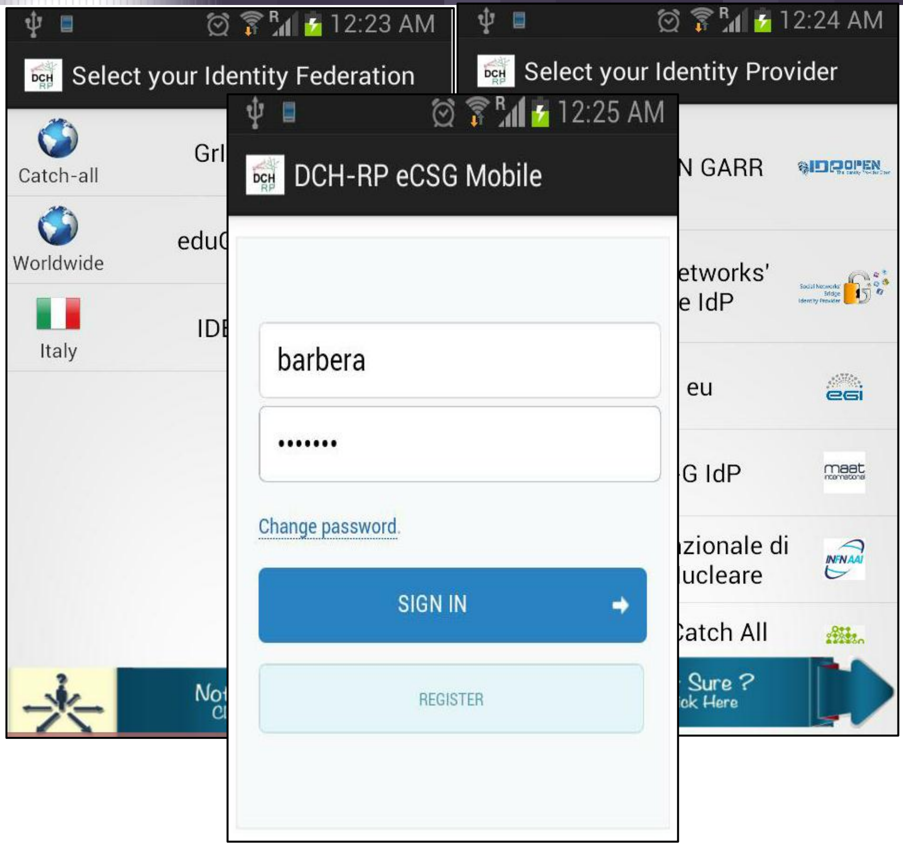
Mobile Support
(Both Android and iOS)



Implementation

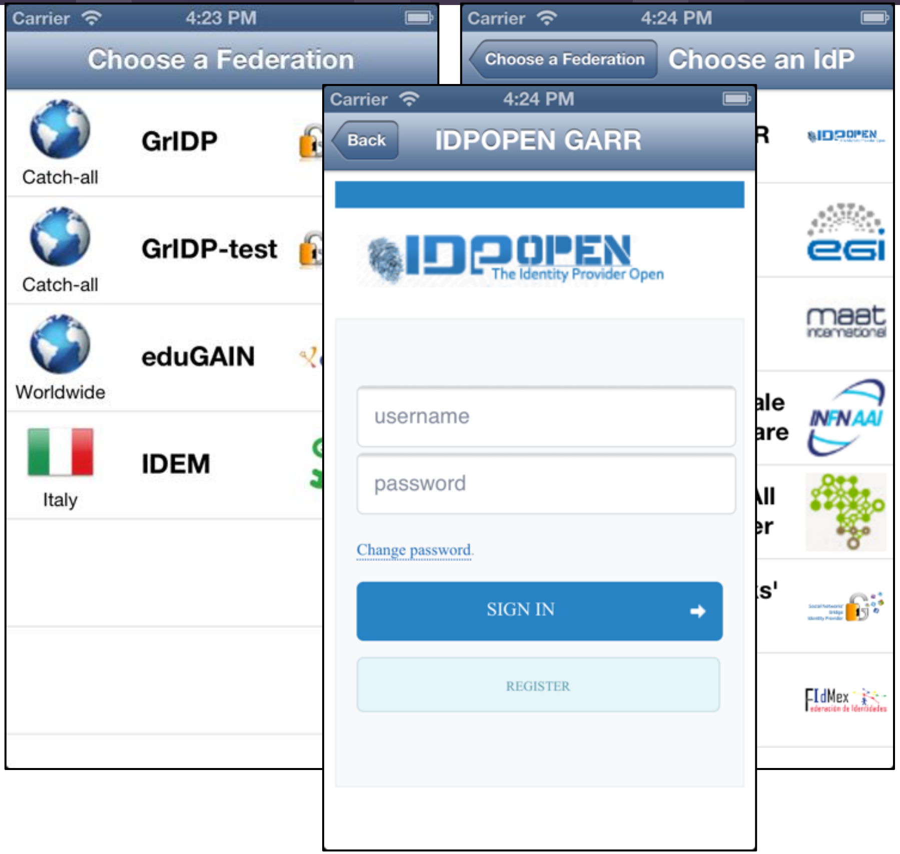
- **Discovery service modified to provide a JSON with federations and IdPs**
  - Based on Shibboleth DS
- **Federations and IdPs selection developed as native apps both for Android and iOS**
- **IdP login page shown in a web view**
  - After the login, the native app catches the SAML token and closes the web view
  - The token is used for the communication with RESTful services

Mobile Authentication



barbera

•••••••



Web views

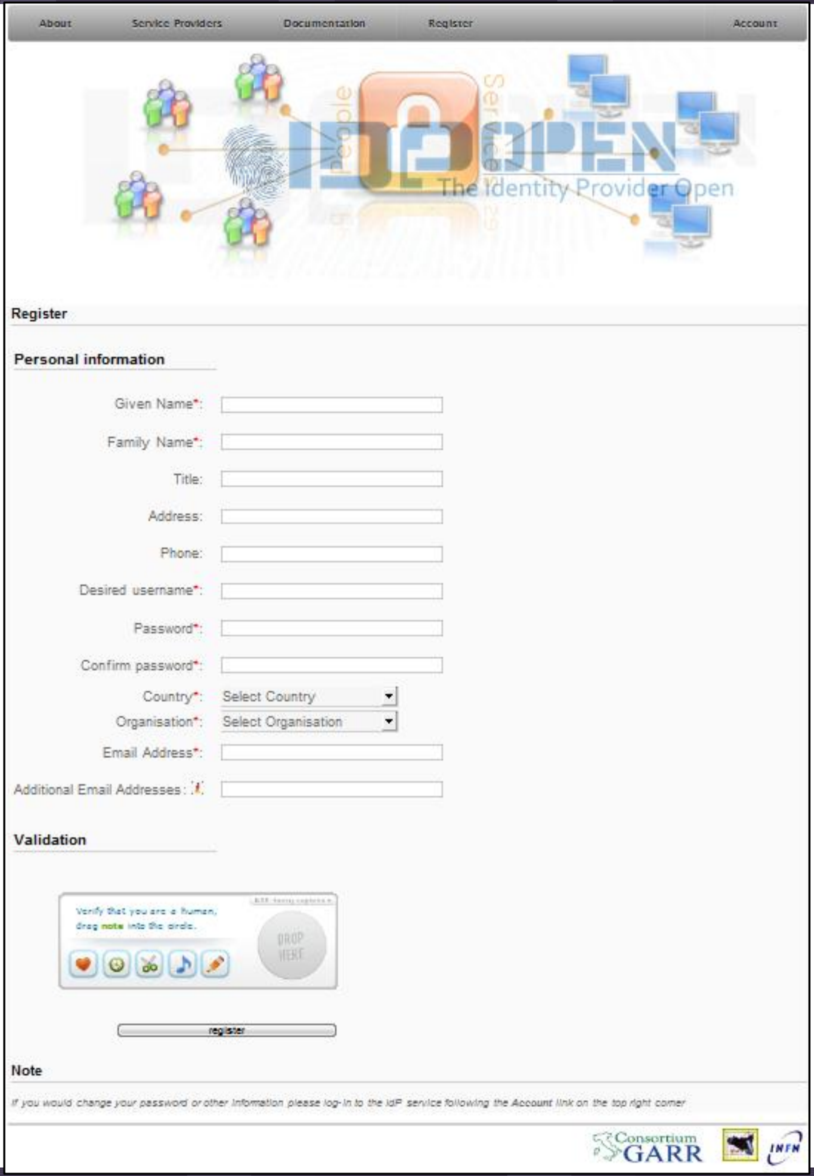
Native apps

IdP Management

- **Catch-all IdP does not have a user DB to access**
  - Users need to ask for registration

- **Anonymous self-registration <u>not</u> supported**

- **A web application has been developed to manage the registration workflow**
  - LDAP as back-end DB



Register

Personal information

Given Name*:

Family Name*:

Title:

Address:

Phone:

Desired username*:

Password*:

Confirm password*:

Country*: Select Country

Organisation*: Select Organisation

Email Address*:

Additional Email Addresses:

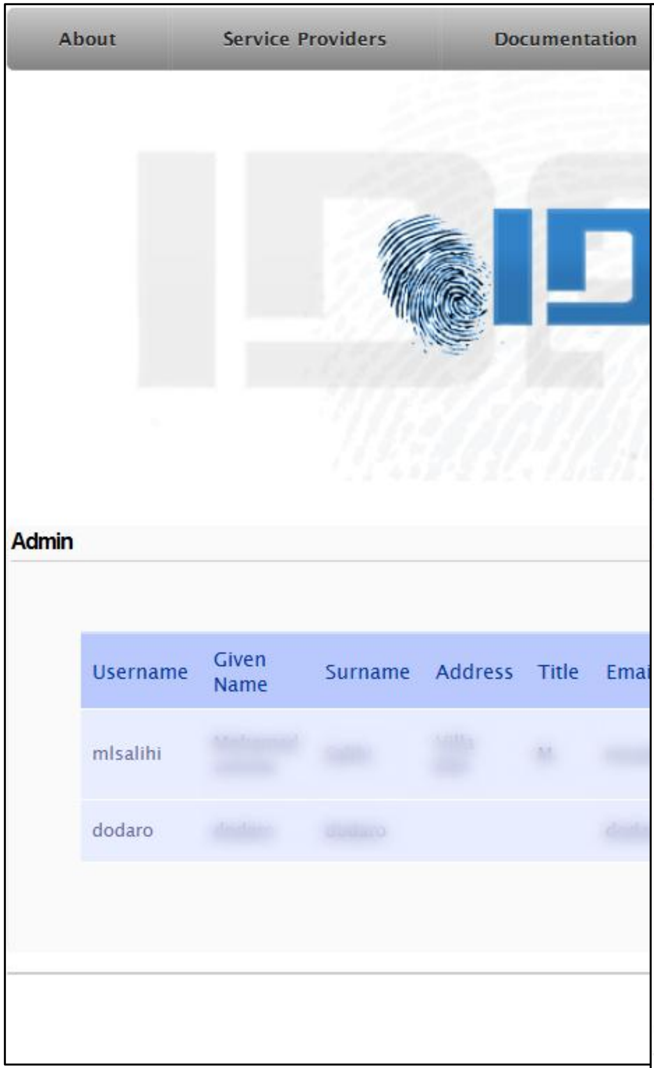
Validation

Verify that you are a human, drag **note** into the circle.

Note

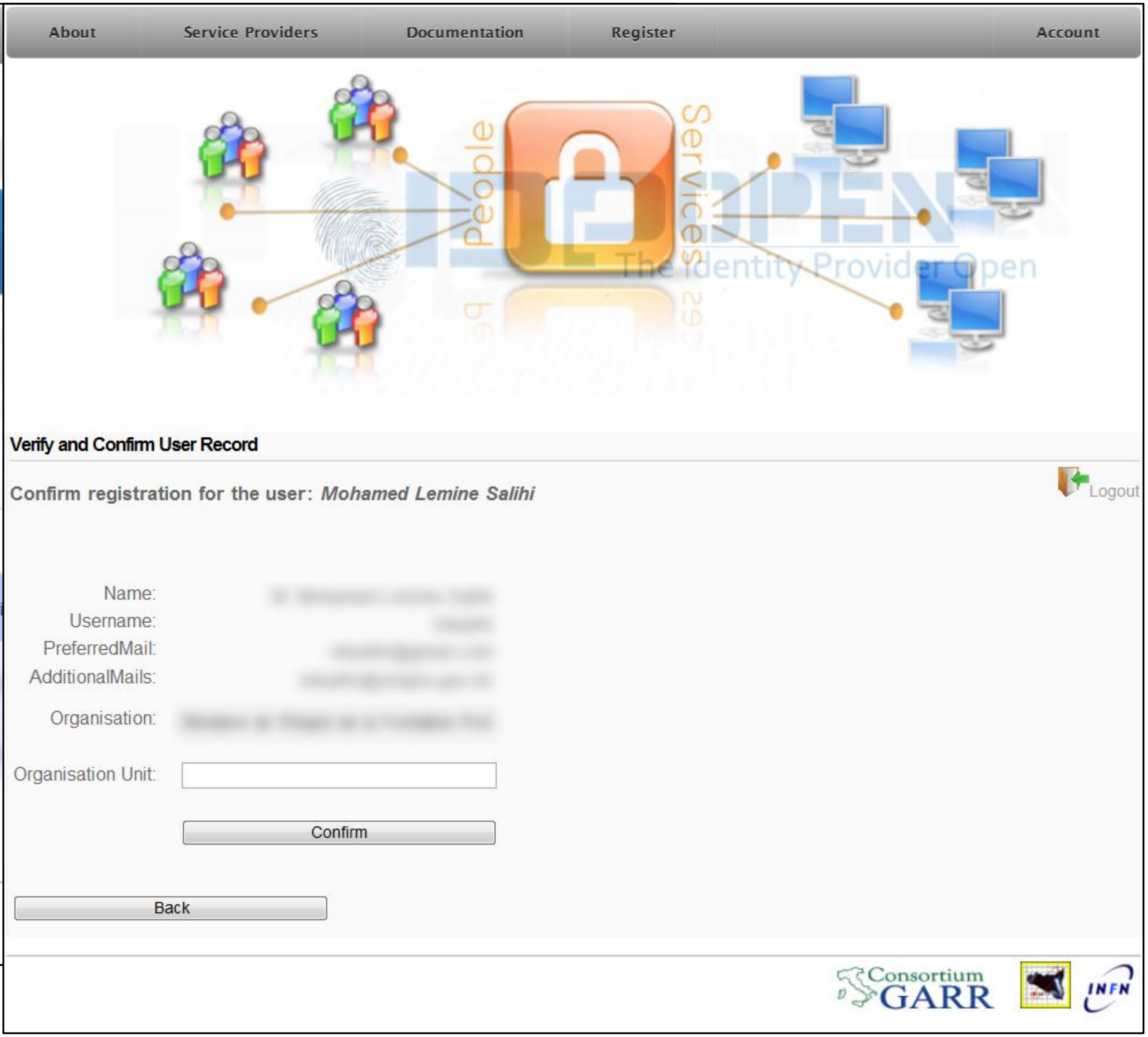
If you would change your password or other Information please log-in to the IdP service following the Account link on the top right corner

IdP Management



Admin

Username	Given Name	Surname	Address	Title	Emai
mlsalihi	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
dodaro	[redacted]	[redacted]			[redacted]

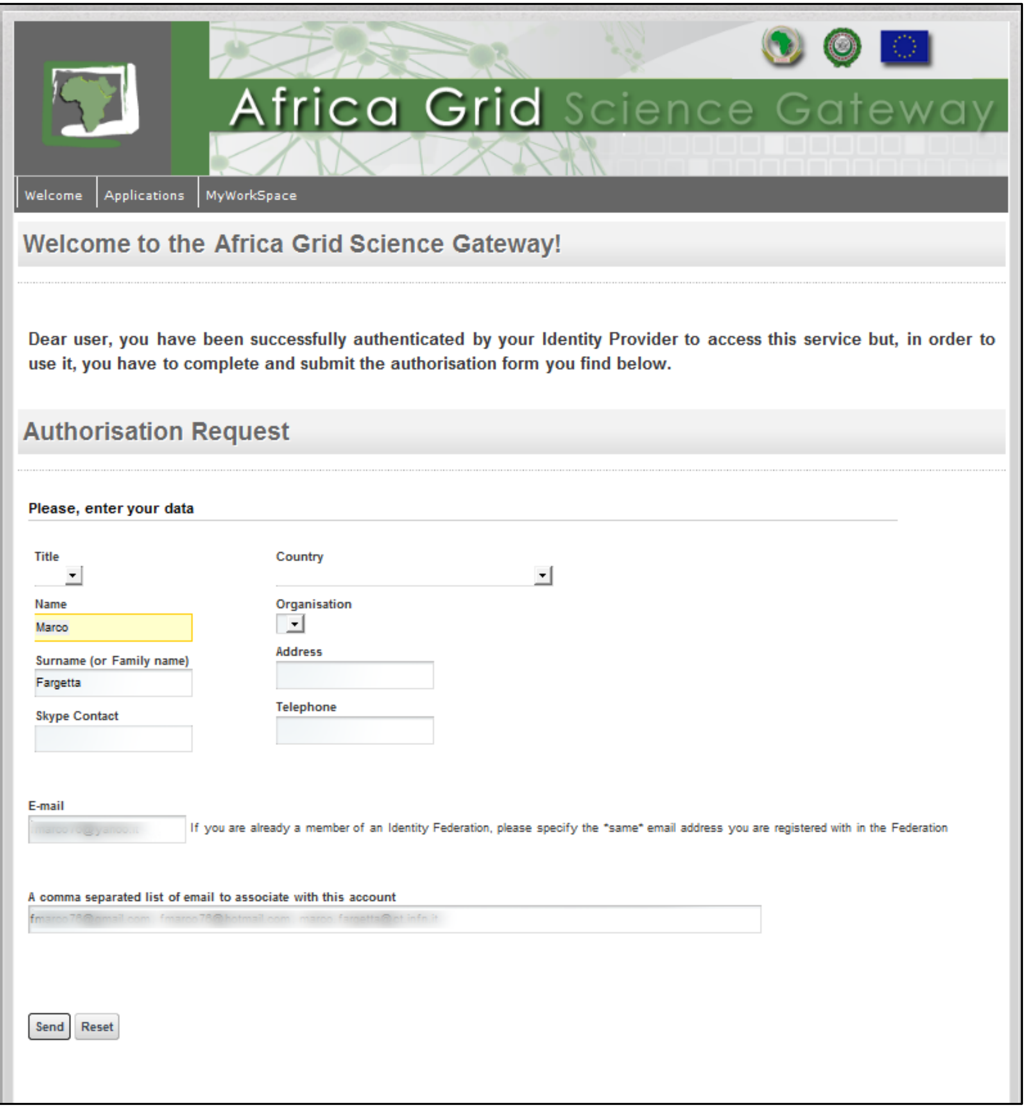


Verify and Confirm User Record

Confirm registration for the user: *Mohamed Lemine Salihi*

Name:	[redacted]
Username:	[redacted]
PreferredMail:	[redacted]
AdditionalMails:	[redacted]
Organisation:	[redacted]
Organisation Unit:	

Science Gateway Authorisation



Welcome to the Africa Grid Science Gateway!

Dear user, you have been successfully authenticated by your Identity Provider to access this service but, in order to use it, you have to complete and submit the authorisation form you find below.

Authorisation Request

Please, enter your data

Title

Country

Name: Marco

Organisation

Surname (or Family name): Fargetta

Address

Skype Contact

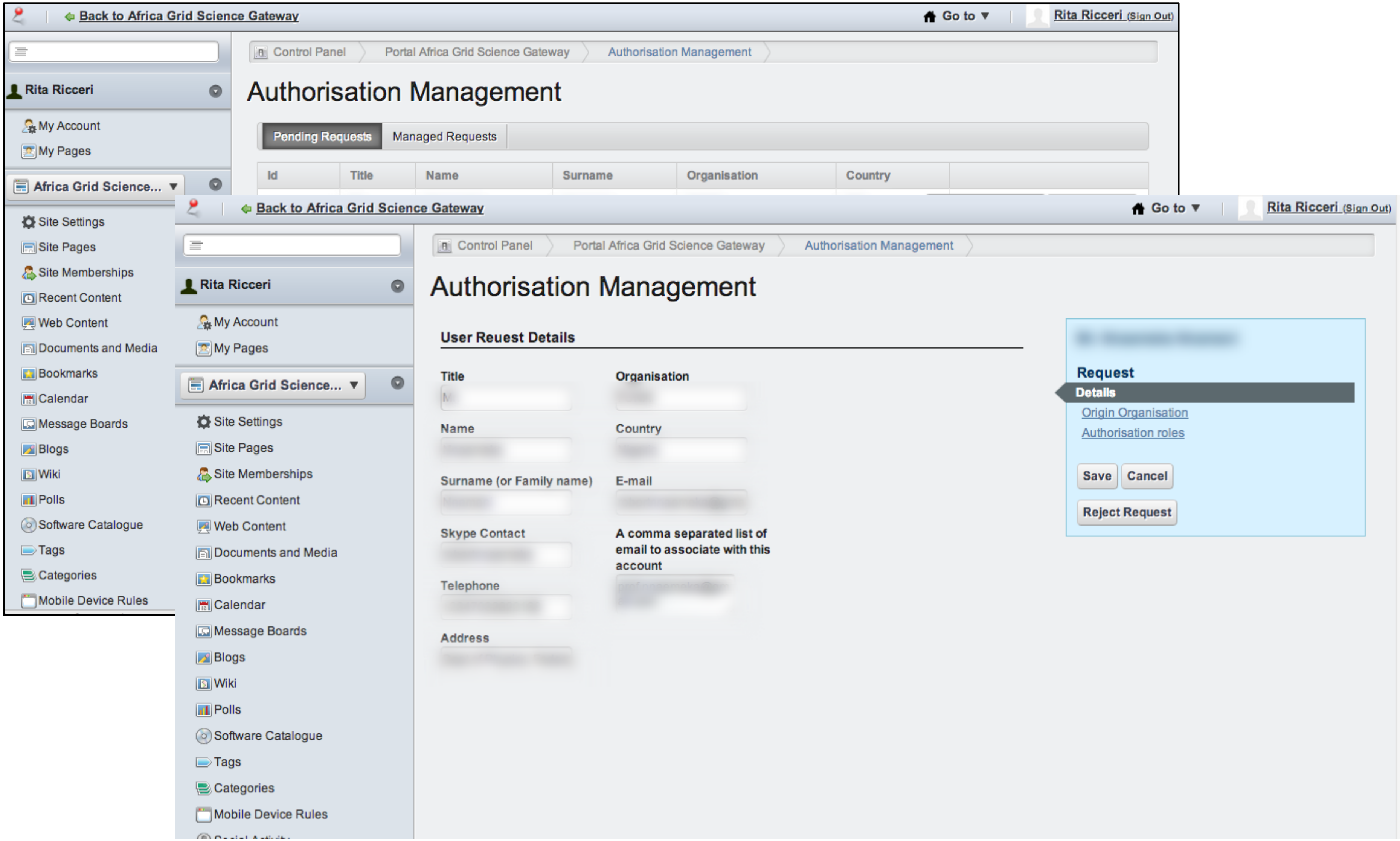
Telephone

E-mail: [redacted] If you are already a member of an Identity Federation, please specify the "same" email address you are registered with in the Federation

A comma separated list of email to associate with this account: [redacted]

- **At first access users are sent to an authorisation request form**
- **Fields are automatically populated with information from SAML token**
  - If not available, users must provide information
- **If different roles are available users can select one or more of them**
  - Users can apply for new roles at any time

Science Gateway Authorisation



Authorisation Management

Id	Title	Name	Surname	Organisation	Country

Authorisation Management

User Reuest Details

Title

Organisation

Name

Country

Surname (or Family name)

E-mail

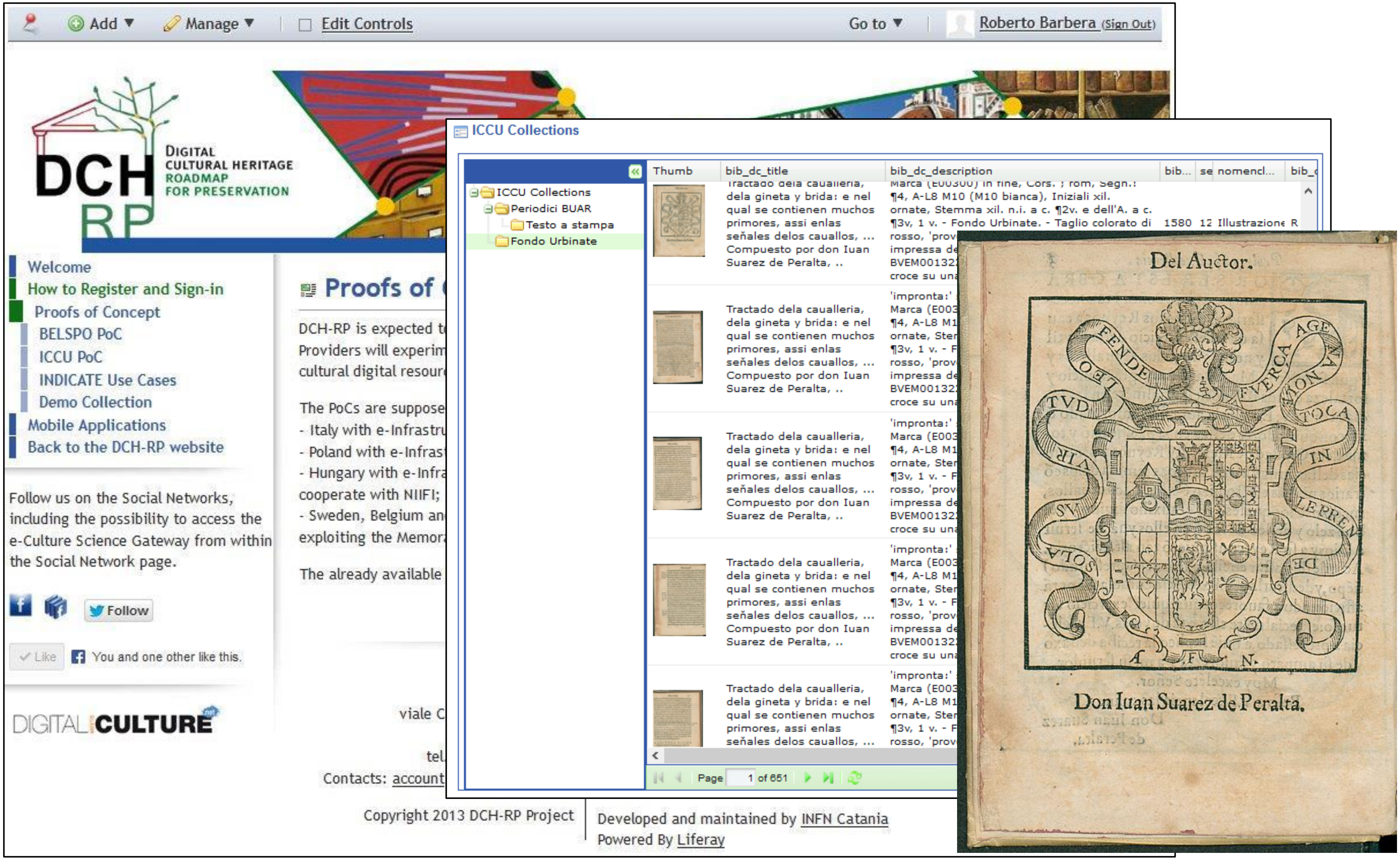
Skype Contact

A comma separated list of email to associate with this account

Telephone

Address

After Signing-in …
… accessing Digital Repositories



Add ▼ Manage ▼ □ Edit Controls Go to ▼ Roberto Barbera (Sign Out)

DCH RP DIGITAL CULTURAL HERITAGE ROADMAP FOR PRESERVATION

- Welcome
- How to Register and Sign-in
- Proofs of Concept
  - BELSPO PoC
  - ICCU PoC
  - INDICATE Use Cases
  - Demo Collection
- Mobile Applications
- Back to the DCH-RP website

Follow us on the Social Networks, including the possibility to access the e-Culture Science Gateway from within the Social Network page.

Follow

✓ Like You and one other like this.

DIGITAL CULTURE

Proofs of

DCH-RP is expected t
Providers will experim
cultural digital resour

The PoCs are suppose
- Italy with e-Infrastru
- Poland with e-Infras
- Hungary with e-Infra
cooperate with NIIFI;
- Sweden, Belgium an
exploiting the Memor

The already available

viale C

tel

Contacts: account

Copyright 2013 DCH-RP Project

Developed and maintained by INFN Catania
Powered By Liferay

ICCU Collections

- ICCU Collections
  - Periodici BUAR
    - Testo a stampa
  - Fondo Urbinate

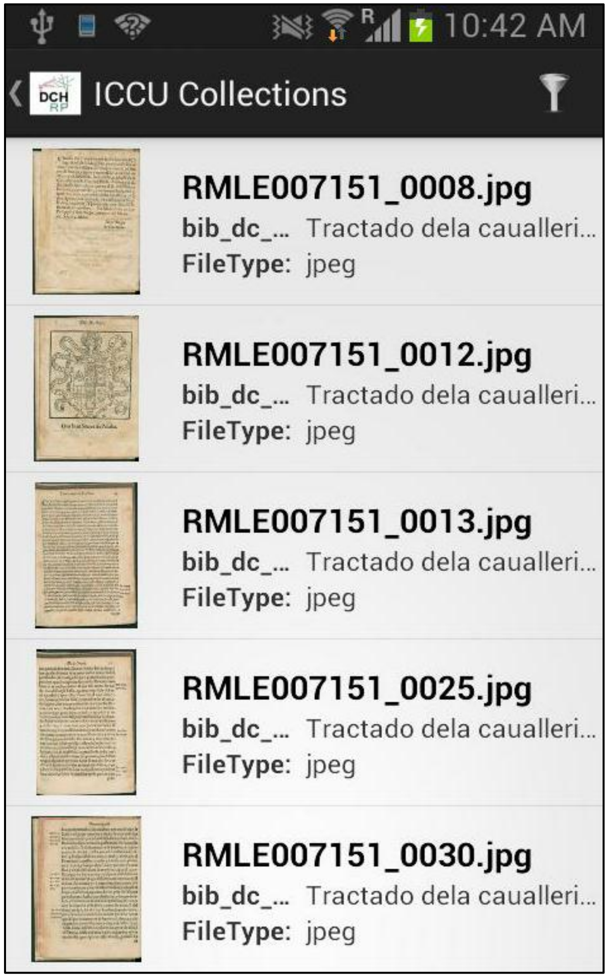
Thumb	bib_dc_title	bib_dc_description	bib...	se	nomencl...	bib_c
	Tractado dela caualleria, dela gineta y brida: e nel qual se contienen muchos primores, assi enlas señales delos cauallos, ... Compuesto por don Iuan Suarez de Peralta, ..	Marca (E00300) in fine, Cors. ; rom, Segn.: ¶4, A-L8 M10 (M10 bianca), Iniziali xil. ornate, Stemma xil. n.i. a c. ¶2v. e dell'A. a c. ¶3v, 1 v. - Fondo Urbinate. - Taglio colorato di rosso, 'prov impressa de BVEM00132 croce su una	1580	12	Illustrazione	R
	Tractado dela caualleria, dela gineta y brida: e nel qual se contienen muchos primores, assi enlas señales delos cauallos, ... Compuesto por don Iuan Suarez de Peralta, ..	'impronta:' Marca (E003 ¶4, A-L8 M1 ornate, Ster ¶3v, 1 v. - F rosso, 'prov impressa de BVEM00132 croce su una				
	Tractado dela caualleria, dela gineta y brida: e nel qual se contienen muchos primores, assi enlas señales delos cauallos, ... Compuesto por don Iuan Suarez de Peralta, ..	'impronta:' Marca (E003 ¶4, A-L8 M1 ornate, Ster ¶3v, 1 v. - F rosso, 'prov impressa de BVEM00132 croce su una				
	Tractado dela caualleria, dela gineta y brida: e nel qual se contienen muchos primores, assi enlas señales delos cauallos, ... Compuesto por don Iuan Suarez de Peralta, ..	'impronta:' Marca (E003 ¶4, A-L8 M1 ornate, Ster ¶3v, 1 v. - F rosso, 'prov impressa de BVEM00132 croce su una				
	Tractado dela caualleria, dela gineta y brida: e nel qual se contienen muchos primores, assi enlas señales delos cauallos, ...	'impronta:' Marca (E003 ¶4, A-L8 M1 ornate, Ster ¶3v, 1 v. - F rosso, 'prov				

Page 1 of 651

Del Auctor.

Don Iuan Suarez de Peralta.

After Signing-in …
… accessing Digital Repositories



10:42 AM

ICCU Collections

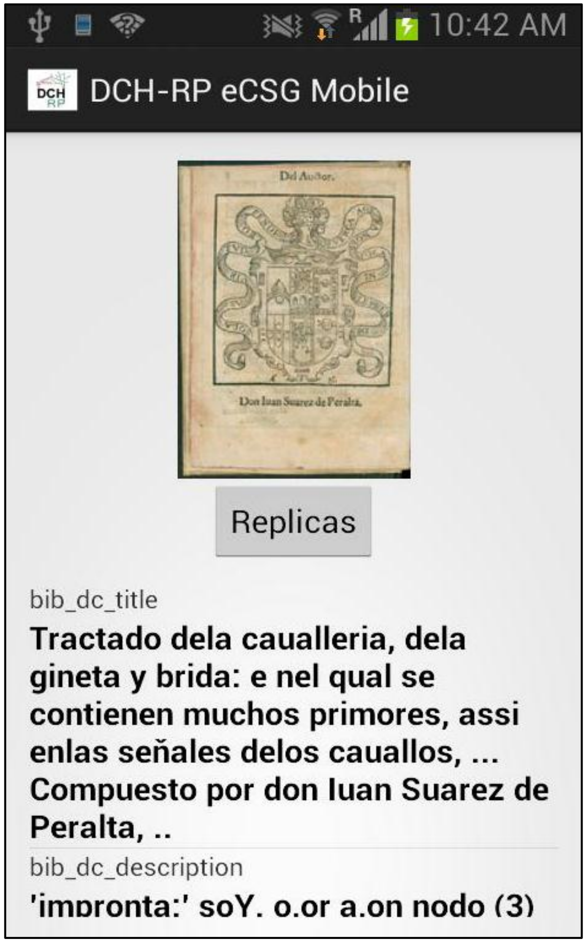
RMLE007151_0008.jpg
bib_dc_... Tractado dela caualleri...
FileType: jpeg

RMLE007151_0012.jpg
bib_dc_... Tractado dela caualleri...
FileType: jpeg

RMLE007151_0013.jpg
bib_dc_... Tractado dela caualleri...
FileType: jpeg

RMLE007151_0025.jpg
bib_dc_... Tractado dela caualleri...
FileType: jpeg

RMLE007151_0030.jpg
bib_dc_... Tractado dela caualleri...
FileType: jpeg



10:42 AM

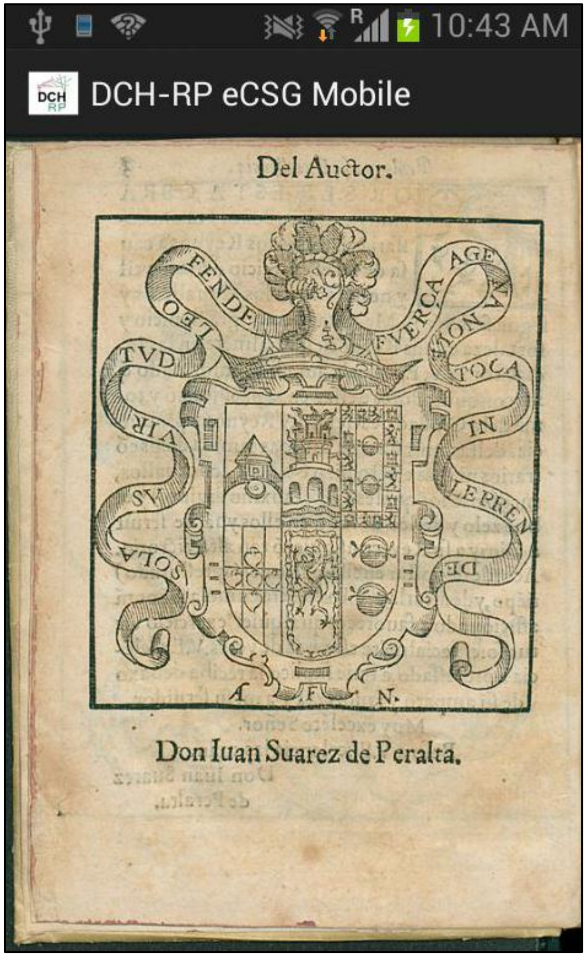
DCH-RP eCSG Mobile

bib_dc_title

Tractado dela caualleria, dela gineta y brida: e nel qual se contienen muchos primores, assi enlas señales delos cauallos, ... Compuesto por don Iuan Suarez de Peralta, ..

bib_dc_description

'impronta:' soY. o.or a.on nodo (3)



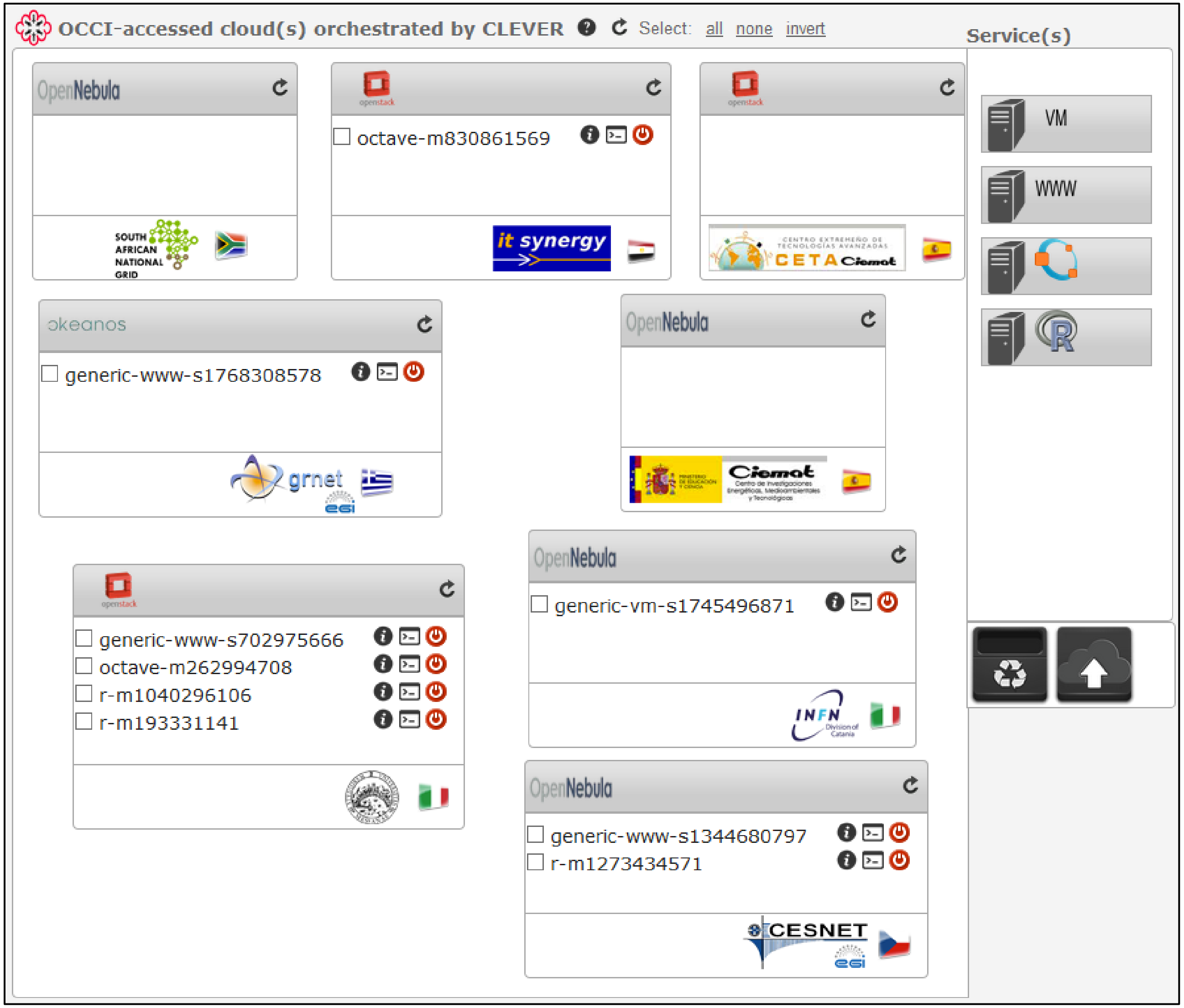
10:43 AM

DCH-RP eCSG Mobile

Del Auctor.

Don Iuan Suarez de Peralta.

After Signing-in …
… managing services in federated clouds



OCCI-accessed cloud(s) orchestrated by CLEVER Select: all none invert

Service(s)

□ octave-m830861569

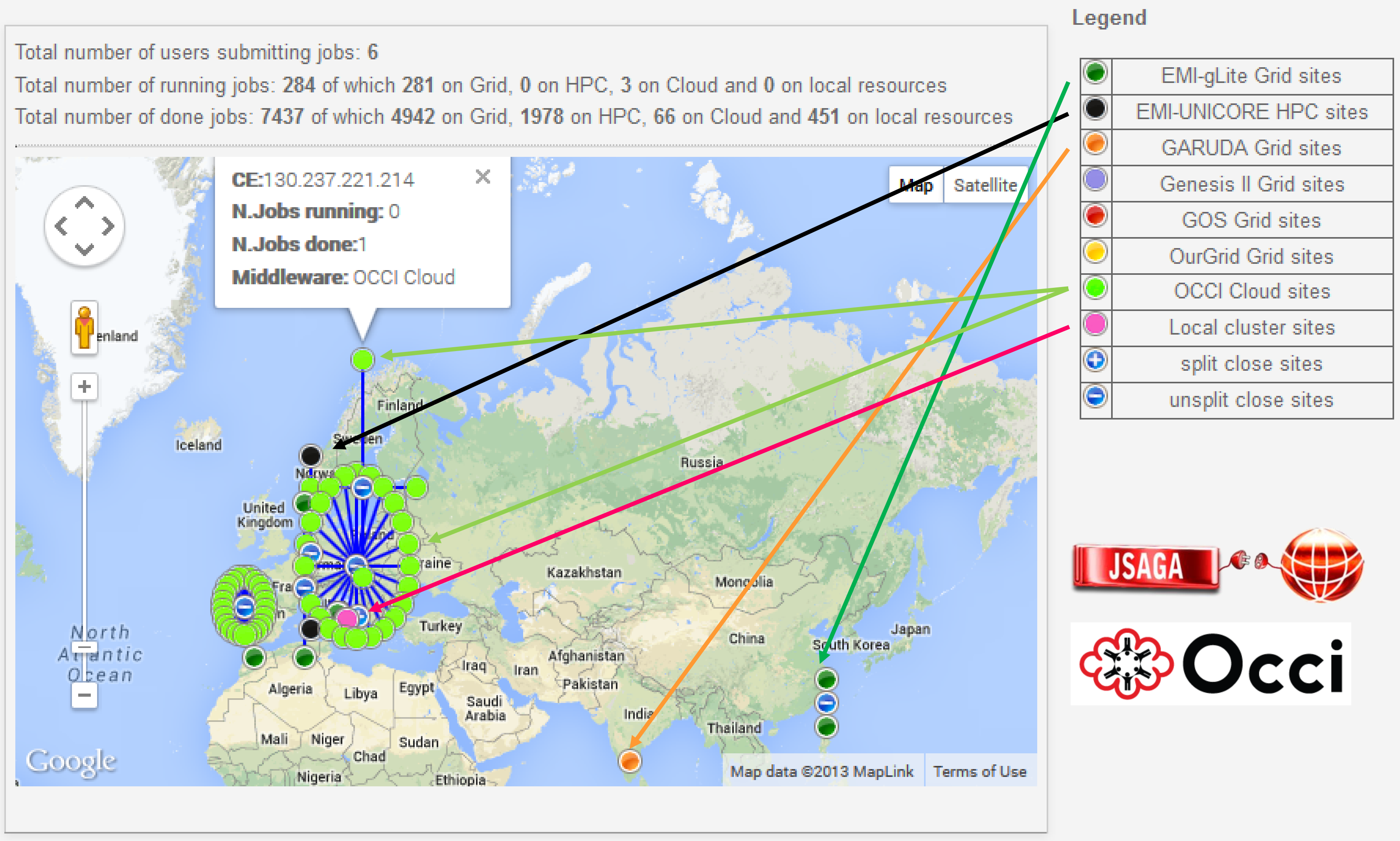
□ generic-www-s1768308578

□ generic-www-s702975666
□ octave-m262994708
□ r-m1040296106
□ r-m193331141

□ generic-vm-s1745496871

□ generic-www-s1344680797
□ r-m1273434571

After Signing-in …
… running jobs on different infrastructures



Total number of users submitting jobs: **6**

Total number of running jobs: **284** of which **281** on Grid, **0** on HPC, **3** on Cloud and **0** on local resources

Total number of done jobs: **7437** of which **4942** on Grid, **1978** on HPC, **66** on Cloud and **451** on local resources

CE:130.237.221.214

N.Jobs running: 0

N.Jobs done:1

Middleware: OCCI Cloud

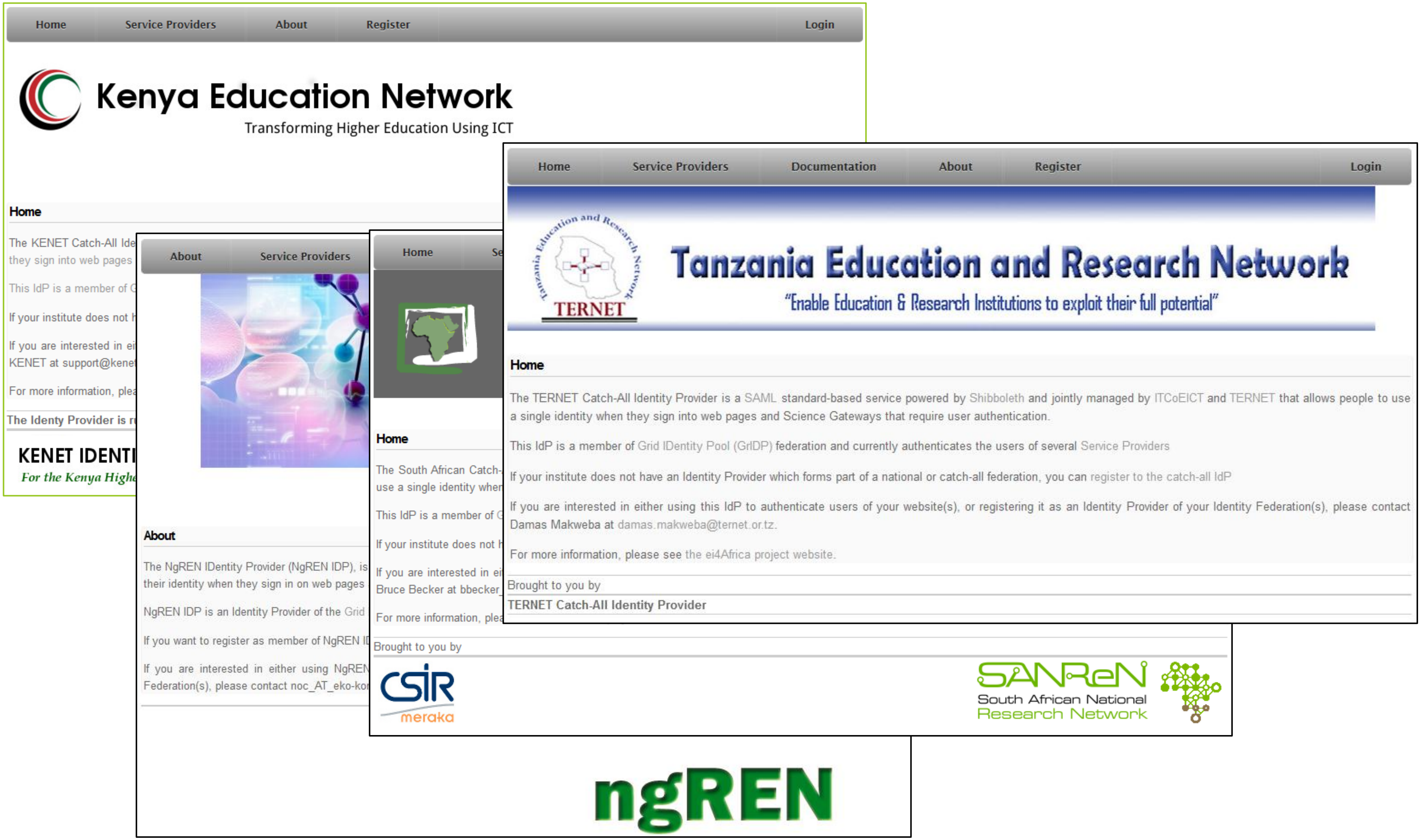
Legend

●	EMI-gLite Grid sites
●	EMI-UNICORE HPC sites
●	GARUDA Grid sites
●	Genesis II Grid sites
●	GOS Grid sites
●	OurGrid Grid sites
●	OCCI Cloud sites
●	Local cluster sites
⊕	split close sites
⊖	unsplit close sites

Support to other organisations

- **Some organisations are deploying SGs using our framework and tools**
  - Including those for authentication/authorisation
- **Federations are not everywhere**
  - Many project partners are located in countries without a national identity federation
  - No know-how on SAML is present
- **We are supporting organisations to deploy their IdPs**
  - They are starting with “catch-all” ones for their local communities

Some of the IdPs supported



Home | Service Providers | About | Register | Login

Kenya Education Network

Transforming Higher Education Using ICT

Home

The KENET Catch-All Ide
they sign into web pages

This IdP is a member of G

If your institute does not h

If you are interested in ei
KENET at support@kenet

For more information, plea

The Identy Provider is r

KENET IDENTI

For the Kenya Highe

About | Service Providers

About

The NgREN IDentity Provider (NgREN IDP), is
their identity when they sign in on web pages

NgREN IDP is an Identity Provider of the Grid

If you want to register as member of NgREN ID

If you are interested in either using NgREN
Federation(s), please contact noc_AT_eko-kon

ngREN

Home | Se

Home

The South African Catch-
use a single identity when

This IdP is a member of G

If your institute does not h

If you are interested in ei
Bruce Becker at bbecker_

For more information, plea

Brought to you by

CSIR meraka

SANReN South African National Research Network

Home | Service Providers | Documentation | About | Register | Login

Tanzania Education and Research Network TERNET

Tanzania Education and Research Network

"Enable Education & Research Institutions to exploit their full potential"

Home

The TERNET Catch-All Identity Provider is a SAML standard-based service powered by Shibboleth and jointly managed by ITCoEICT and TERNET that allows people to use a single identity when they sign into web pages and Science Gateways that require user authentication.

This IdP is a member of Grid IDentity Pool (GrIDP) federation and currently authenticates the users of several Service Providers

If your institute does not have an Identity Provider which forms part of a national or catch-all federation, you can register to the catch-all IdP

If you are interested in either using this IdP to authenticate users of your website(s), or registering it as an Identity Provider of your Identity Federation(s), please contact Damas Makweba at damas.makweba@ternet.or.tz.

For more information, please see the ei4Africa project website.

Brought to you by

TERNET Catch-All Identity Provider

Implementation and status

- **IdPs deployed use the same tools and web application of our catch-all IdP**
  - They use Shibboleth, LDAP and the web application developed by INFN Catania for user management
- **3 IdPs currently under test and 1 already included in the GrIDP federation**
  - Some NRENs are also planning to create their federation and add more IdPs
- **IdPs for own users are also foreseen in the short term**

Summary

- **Identity federations make authentication on distributed systems easy and safe**
  - Still many organisations are not federated and tools for not-federated users are needed
- **We built a catch-all federation and IdPs**
  - Catch-all IdPs important for services whose users are distributed in many countries and belonging to many organisations
- **Many organisations supported to implement their services (IdPs and SGs)**
  - Tools for user management could be integrated in the main SAML implementations (e.g. Shibboleth)

Outlook

- **Finalise the deployment of IdPs and integrate them the in GrIDP federation**
- **Foresee the use of SAML for the authentication to clouds**
  - – OpenStack based clouds allow the use of SAML
- **Investigate the integration with OAuth protocol for mobile authentication and authorisation**
  - – Current approach has several limitations

THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
DANKSCHEEN
BİYAN
SHUKRIA
TINGKI
YAQHANYELAY
CHALTU
NUHUN
SPASSIBO
SNACHALHUYA
TASHAKKUR ATU
YUSPAGARATAM
WABEEJA
MAITEKA
HUI
SUKSAMA
DHANYABAAD
ANIHA
EKHMET
MERSI
SPASIBO
DENKAUJA
NENACHALHYA
UNALCHÉESH
GUI
HATUR
EKOJU
SIKOMO
MAKETAI
ATTO
SANCO
MERASTAWHY
GAEJTHO
KOMAPSUMNIDA
MAAKE
GRAZIE
MEHRBANI
PALDIES
LAH
TAVTAPUCH
MEDAWAGSE
JUSPAXAR
BAIIKA
GOZAIMASHITA
EFCHARISTO
AGUYJE
FAKAAUE
BOLZÏN
MERCI
MINMONCHAR