

Autorizzare gli utenti delle Federazioni di Identità sulle e-infrastrutture mediante gli Science Gateway

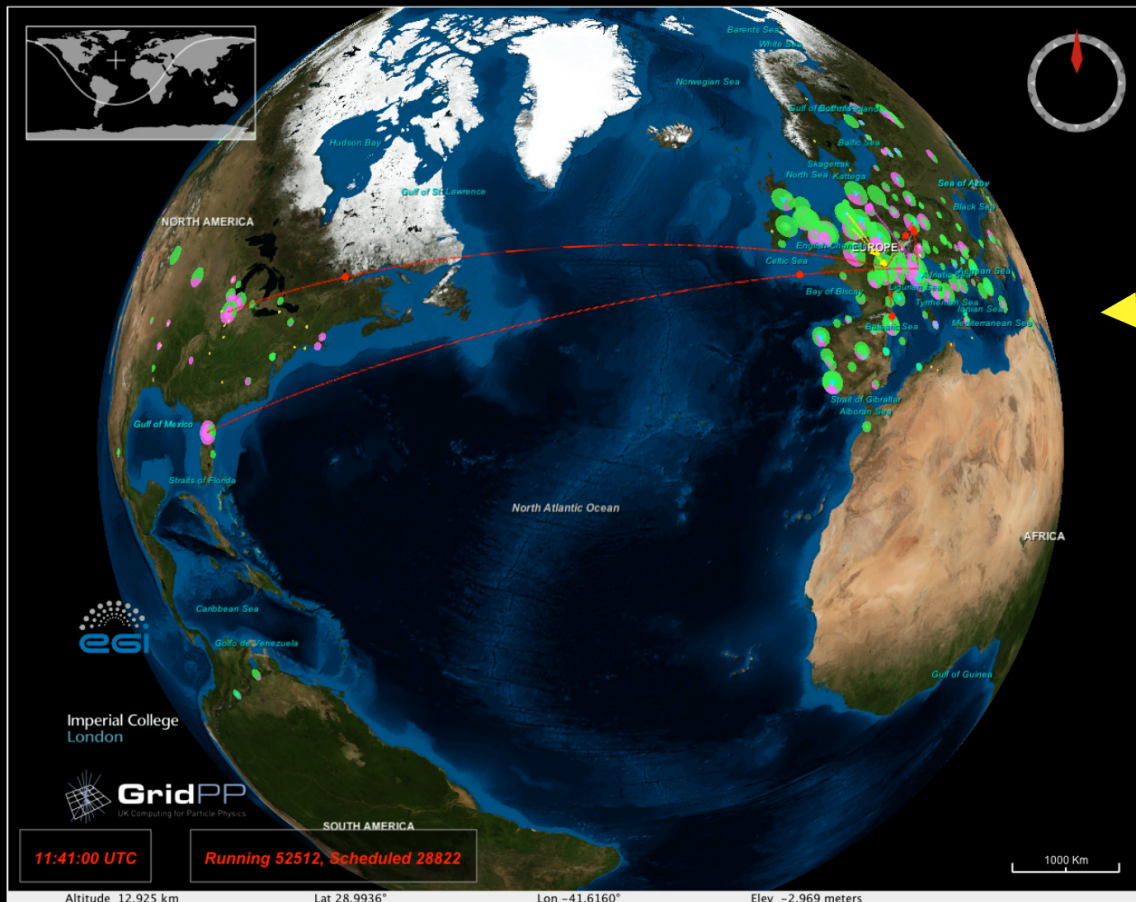
Marco Fargetta

INFN Catania & Consorzio COMETA

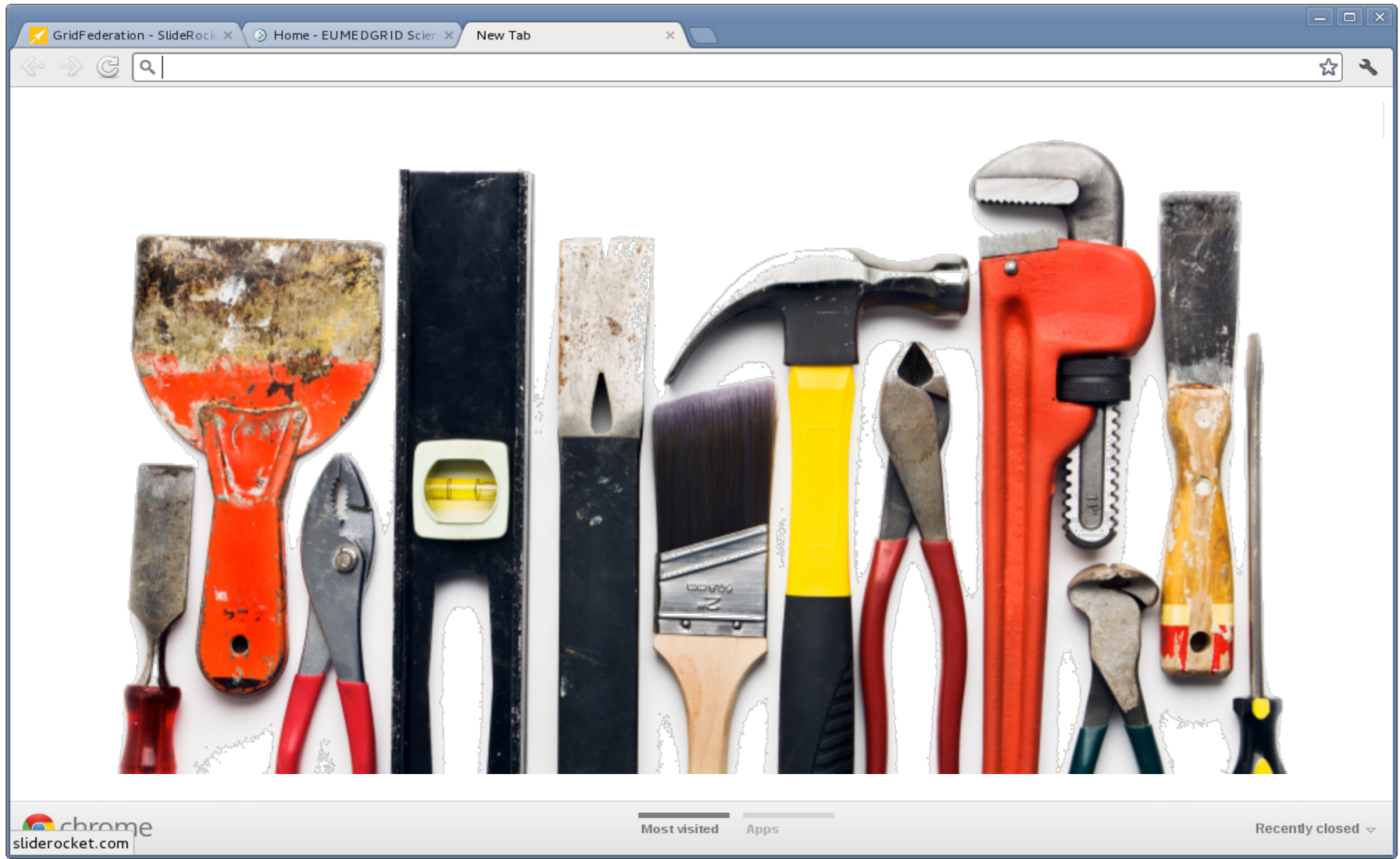
Grid Computing allows users to access and use a huge number of computers spread around the world



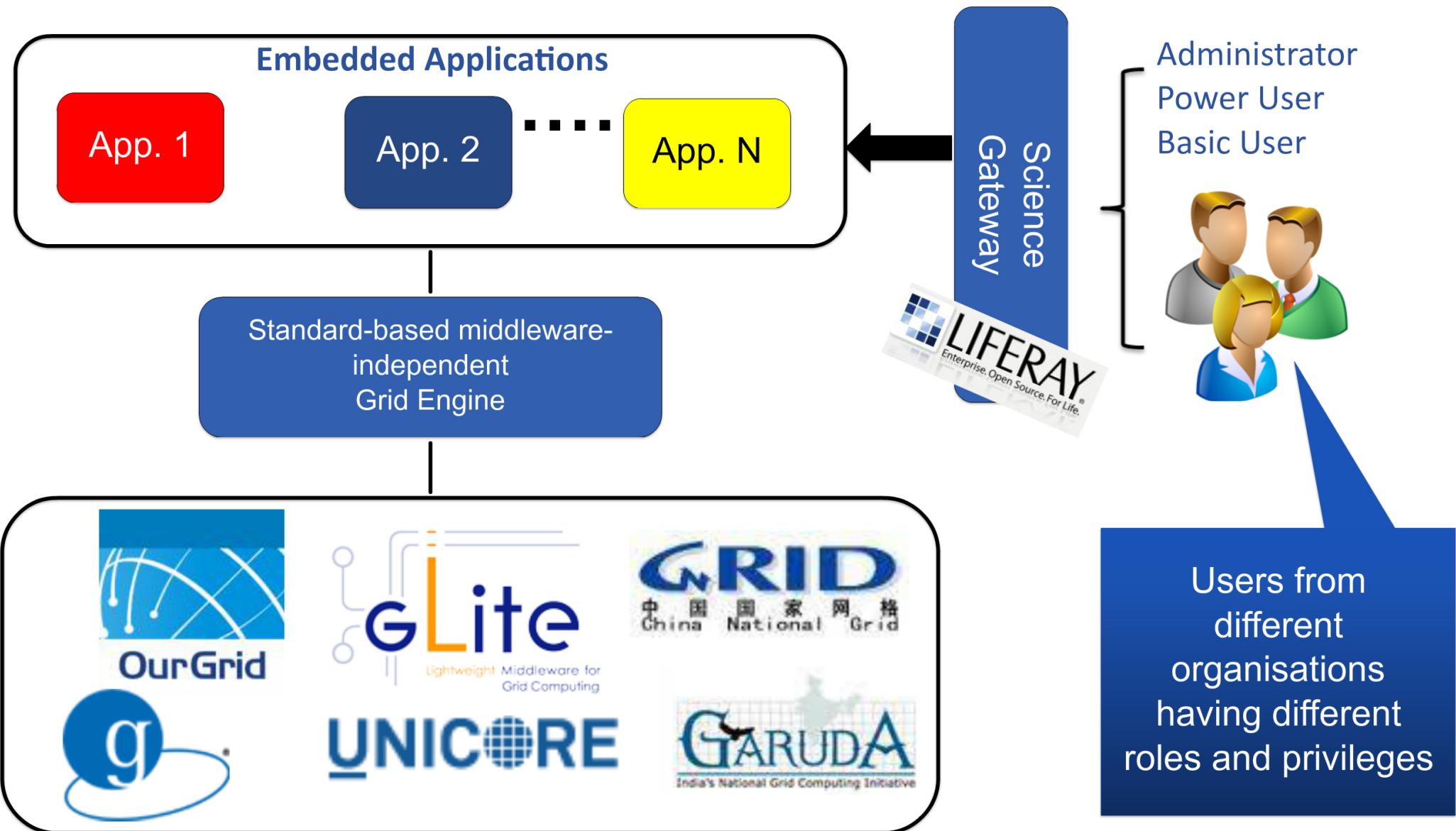
GRID



Community-driven web portals have started to integrate Grid Tools and Applications



Catania Science Gateway reference model



**The distributed/
cross-domain
nature of **Grid**
requires strong
security
mechanisms**



**Users struggle to
comply with Grid
complex security
rules for certificate
management**



Simple access



Users would
access and use
Grid resources
such as any other
web service
available in their
organisations



Identity Federations
provide the requested
security

Grid users distributed
around the world

Grid



Many Federations and other identity sources integrated together but with **different trust level**

Users willing to access the services using
social identities need to be identified

Identities verified
in person



The SP security is based on **Shibboleth** module for apache web server




Science Gateways use **Liferay**
Portal Application Framework



**The mail attribute used to
associate federated identities with
local identities**

Other attributes not well supported in Liferay

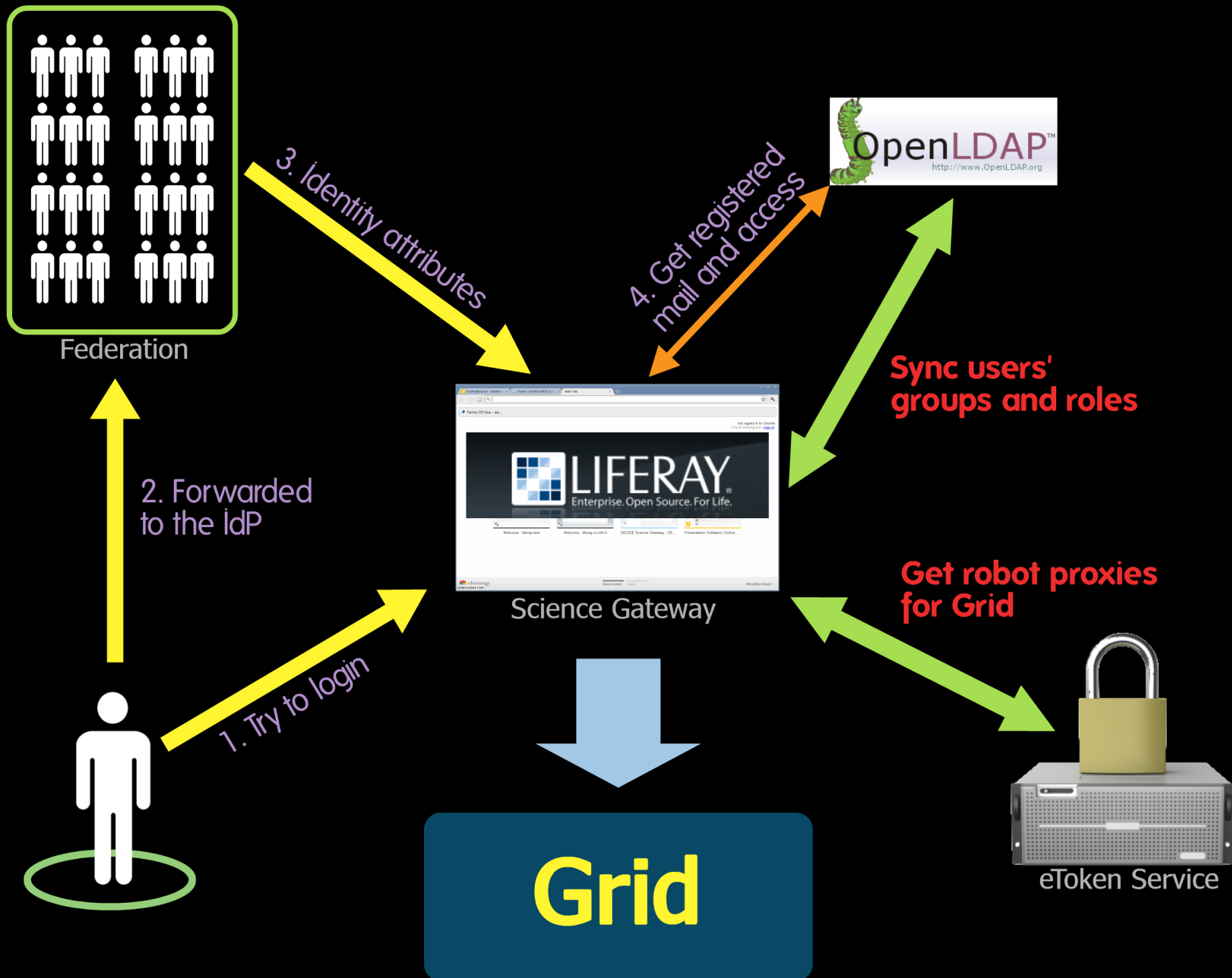
A silhouette of a baby in a white dress standing in a room with large windows and wooden chairs. The baby is in the center, facing slightly left. To the left, an adult's legs and hands are visible. To the right, another adult's legs and a chair are visible. The room has a wooden floor, a striped rug, and large windows in the background.

The first step for users accessing the SP is to explicitly request a local account and one or more roles



Under development a mechanism
for the automatic account creation
according to SAML attribute

Its use depends on the Science Gateway reference community



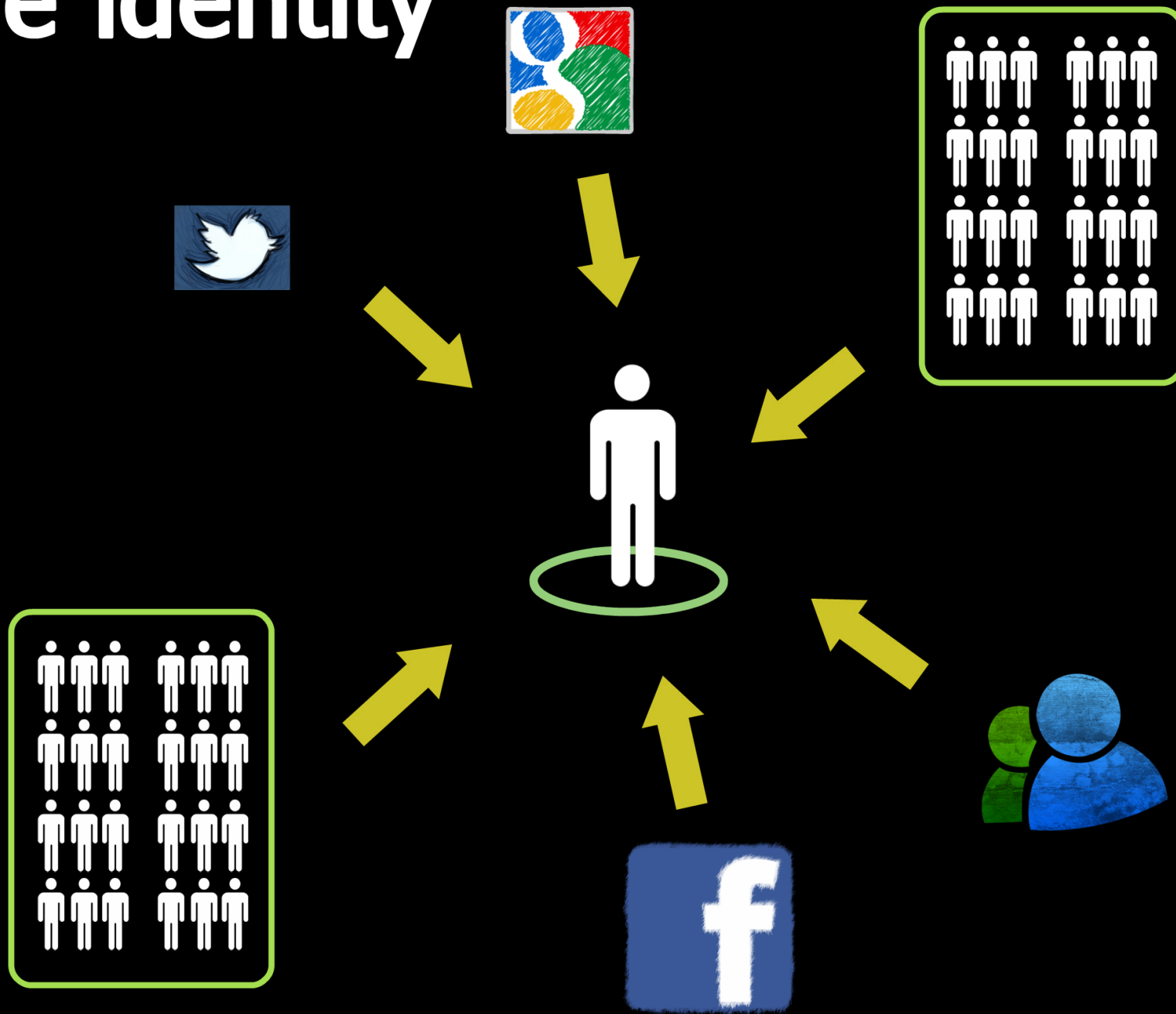


**Identity Federations truly
simplify users authentication**

**Problematic authorisation in
some cases**

**Some features missed or not well
documented**

One identity



A list of e-mails associated with a
user allows to use multiple
Identity Providers

*Users may continue their activities moving
across organisations*

Metadata filter should allow to
dynamically skip IdPs
according to the provided
attributes

Users should see only working IdPs

*Manual check and blacklist inclusion of
IdPs not viable*

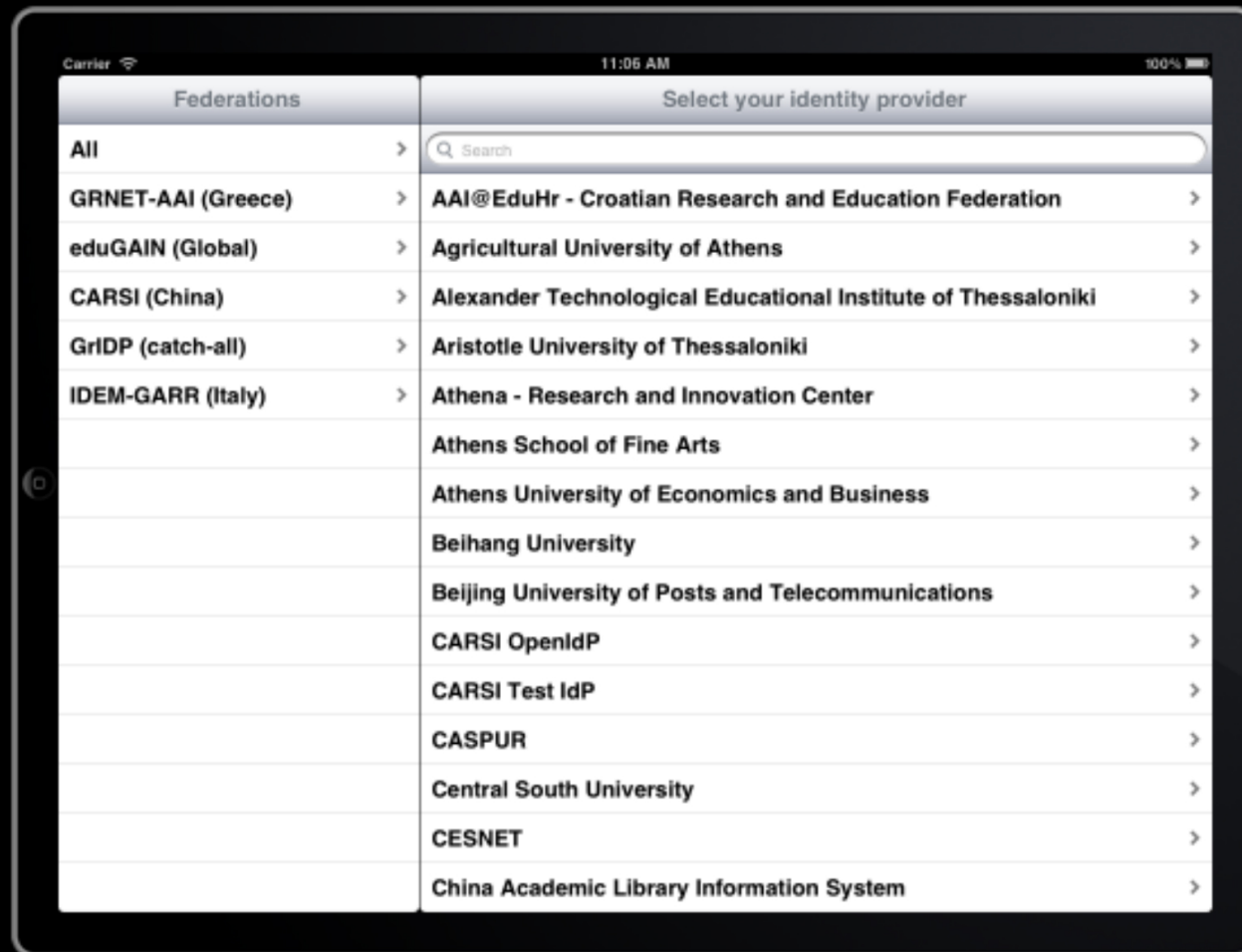
Attributes should better **describe
the user activity** and not only the
position in the organisation for a
more automatic authorisation
system



Support for authentication
delegation needs improvement
to allow services authentication
on behalf of users



Authentication in mobile Apps feasible but not easy to implement



14 SGs already deployed

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

CHAIN

COGITO-MED

DECIDE

EarthServer

EUMEDGRID

GARR

GILDA

GISELA

INDICATE

KLIOS

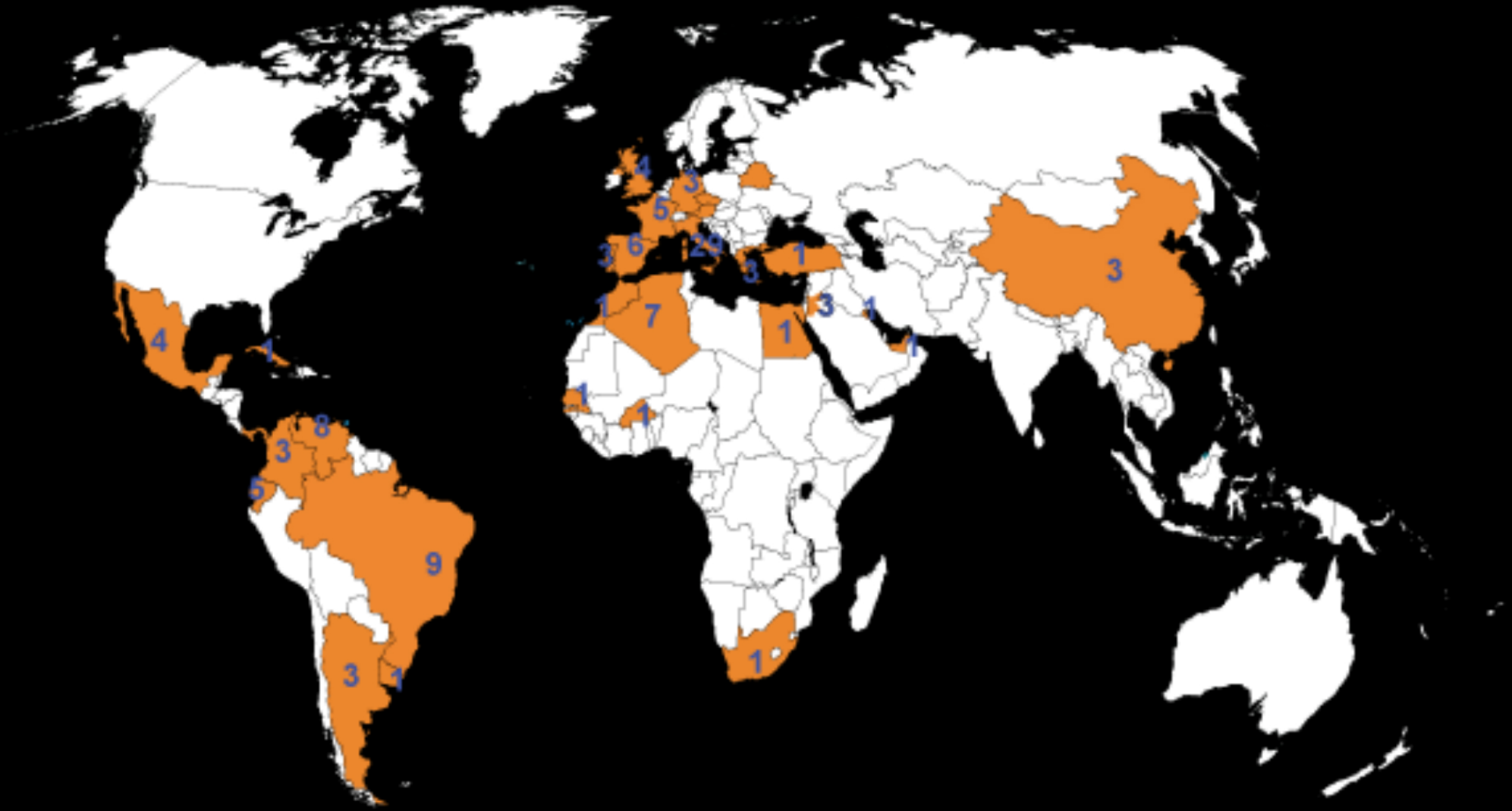
RICEVI

SG to IGI

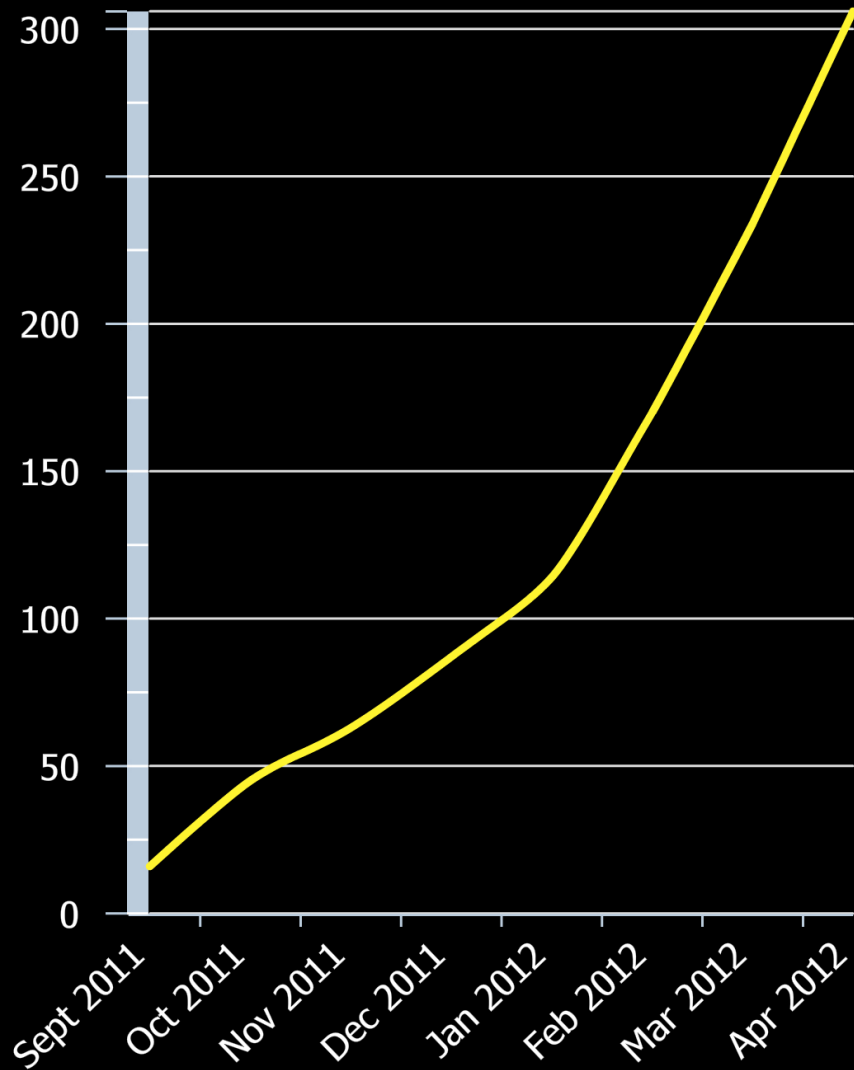
SPECIAL

ViralGrid

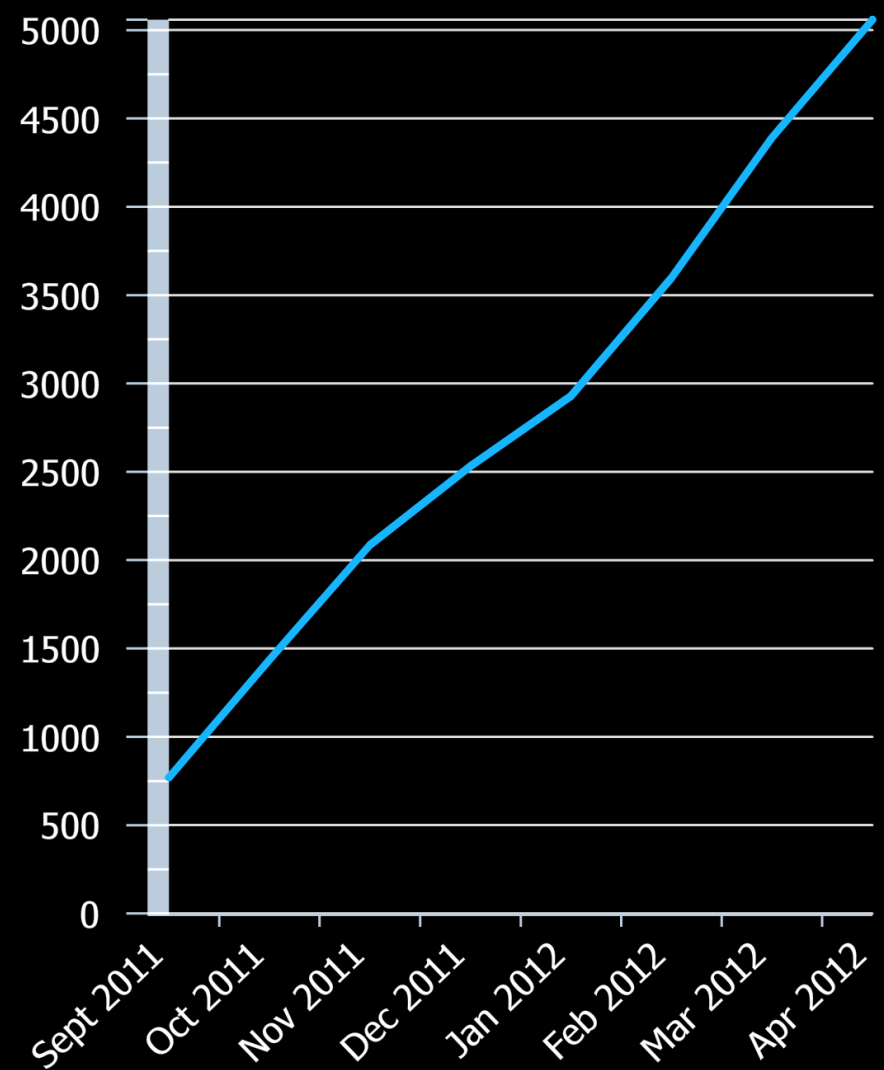
Users from 114 Organisations in 31 Countries



Registered users



User sign-ins





"Authentication and authorisation schema: very useful to allow users to access GISELA infrastructure without a digital certificate"

- Bernard Marechal, GISELA Project

"The Auth and AuthZ to access the Science Gateway (gw.ct.infn.it) are very easy to understand and does not require any additional plugins and client software."

- Massimo Rizzi, ARCEM

"The authentication and authorisation schema presents some problems at first for developers, although the schema is significantly easier for the end user than the usual scheme used in other GRID"

- Luis A. Nuñez, Universidad Industrial de Santander

"Users' feedback very positive: applications are very easily accessed and used"

- Fulvio Galeazzi, DECIDE Project

"It is really great having a catch-all Federation run by INFN Catania"

- D. Vicinanza, DANTE/ASTRA and LSO

"Authentication and authorisation schema – easy to use and understand"

- Antonella Fresa, INDICATE Project

Identity federations tools have a **steep learning curve** for administrators but allow to implement a very secure user access to web resources **easy to maintain**

Deploy with other tools or in more complex scenarios (e.g. mobile apps, delegation) is **not trivial**



Support of **mobile device** will be improved
for both web and native apps

Some SGs will **integrate a SAML based
authorisation mechanism**



People involved

M. Fargetta
(COMETA)

R. Ricceri
(INFN)

R. Barbera
(INFN/COMETA)

B. Monticini
(GARR)

S. Monforte
(INFN)

A. Calanducci
(COMETA/EtnaTraining)

M.L. Mantovani
(GARR)

E. Ingrà
(GARR)

R. Rotondo
(GARR)

G. La Rocca
(INFN)



THANK YOU

GRACIAS
ARIGATO
SHUKURIA
JUSPAXAR

DANKSCHEEN
SHUKRIA
BiYAN

TASHAKKUR ATU
YAQHANYELAY
SUKSAMA
EKHMET
MEHRBANI
GRAZIE
MAAKE
KOMAPSUMNIDA
GOZAIMASHITA
EFCHARISTO
BOLZİN
MERCI

SPASSIBO
SNACHALHUYA
NUHUN
CHALTU
WABEEJA
MAITEKA
HUI
YUSPAGARATAM
UNALCHEESH
SPASIBO
DENKAUJA
NENACHALHYA
ATTO
ANHA
DIANYADAAD
SAHCO
MERASTAWHY
GAEJTHO
AGUYJE
FAKAAUE
LAH
TINGKI
HATUR
GUI
EKOJU
SIKOMO
MAKETAJ
MIMMONCHAR