



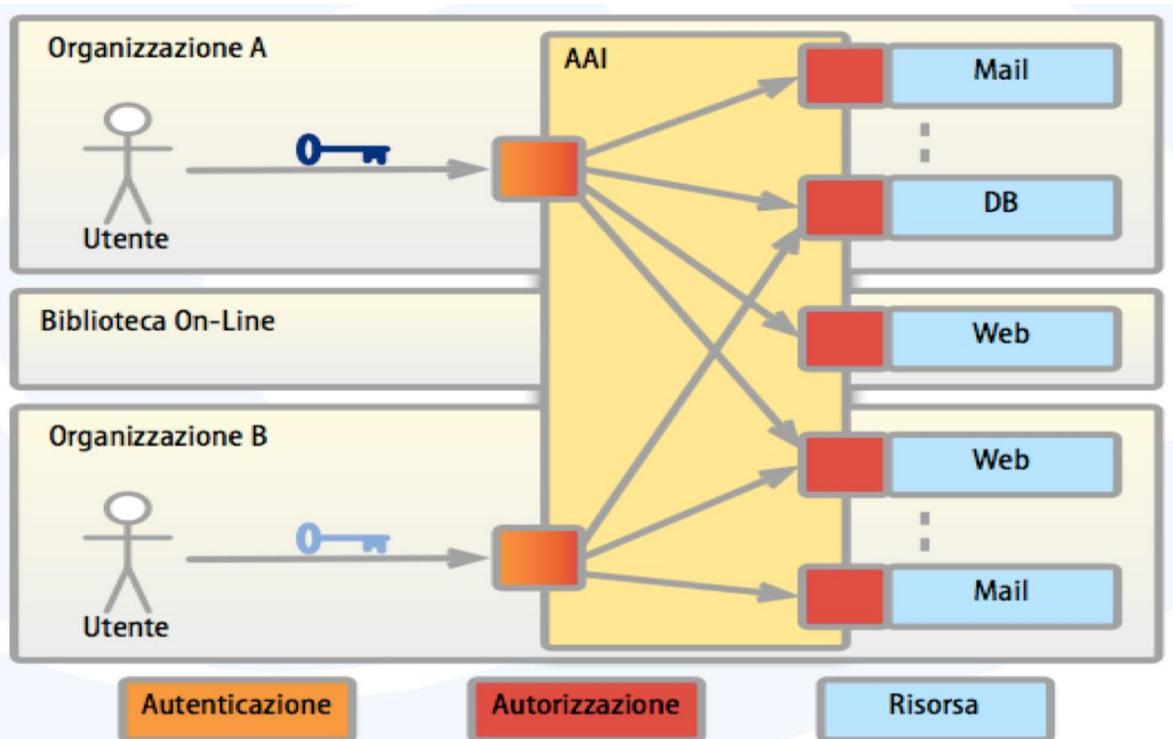
Franco Tinarelli
INAF – IRA

AdR Bologna
16/12/2014

Infrastrutture di Autenticazione e Autorizzazione

- **IDEM (Identity Management per l'accesso federato)** è il nome della **Federazione Italiana di Autenticazione e Autorizzazione** delle Organizzazioni che appartengono alla Comunità GARR.
- La Federazione è formata dagli IdP (Identity Providers) degli Enti GARR (CNR, INFN, INAF, ENEA, Università' etc.) e dagli SP (Service Providers) appartenenti alla stessa comunità' GARR, a Istituzioni e società' esterne, nazionali e internazionali.
- Scopo della Federazione: fornire un servizio di Single Sign-On (SSO) per l'utilizzo dei servizi federati

- Uniche Credenziali per piu' Servizi Federati



- Membro della Federazione che gestisce la registrazione dei propri Utenti, ne mantiene le informazioni e fornisce un meccanismo di autenticazione, è responsabile degli Attributi forniti per ciascuno di essi.
- CNR e INAF partecipano alla Federazione con un proprio IdP.
- L'autenticazione avviene tramite l'inserimento di Username e Password (tipicamente gestite da un server LDAP).
- L'autorizzazione all'utilizzo di un servizio avviene tramite il rilascio di attributi conservati nello stesso server di autenticazione o presso DB esterni.

- Membro della Federazione che mette a disposizione un servizio, tipicamente una applicazione web.
- L'accesso al servizio attiva la catena di Autenticazione/Autorizzazione.
- Il servizio viene offerto solo ricevendo tutti gli attributi richiesti.

GARR VCONF



GARR/CINECA



ePTID (R), ePSA (R), sn (R),
givenName (R), mail (R)

- Per ottenere l'autenticazione attraverso l'identity provider di INAF e' indispensabile configurare la propria password sul server LDAP dell'Ente. I passi necessari per farlo sono semplici e completamente automatizzati, si parte dalla URL <https://www.ced.inaf.it/idem-info/> e si sceglie dal menu di sinistra la voce "CREDENZIALI DEGLI UTENTI". Per INAF la UserID è **cognome.nome**
- Il CNR Amministrazione Centrale (esistono anche IdP di singoli Istituti e Sedi) usa per l'autenticazione le credenziali **SIPER** e la UserID degli utenti è **nome.cognome**

Trovare Servizi in IDEM

- La pagina web di IDEM <http://www.idem.garr.it> fornisce un elenco dei fornitori di servizi (SP) e dei fornitori d'Identità (IdP).

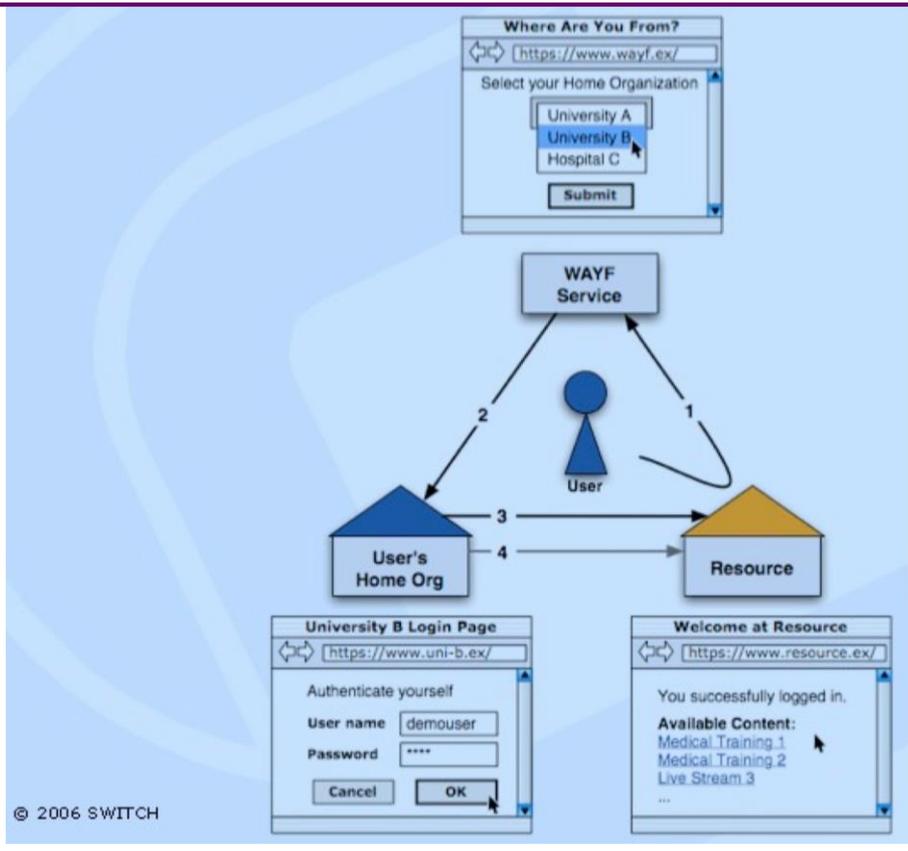
Partecipanti	CNR	CNR Amministrazione Centrale		
Servizi				
Servizi di gestione e verifica delle identità				
Risorse				
Informazioni Tecniche	GARR VCONF	GARR/CINECA		ePTID (R), ePSA (R), sn (R), givenName (R), mail (R)

Annotations:

- Blue arrow from **Servizi** to **Link al Servizio**
- Blue arrow from **Risorse** to **GARR VCONF**
- Blue arrow from **Informazioni IdP** to the top row
- Blue arrow from **informazioni SP** to the bottom row
- Blue arrow from **Attributi** to the bottom row
- Blue double-headed arrow between **Sito web dell'Ente** and the bottom row

Lo schema di A&A

- 1) L'utente accede alla risorsa web, il service provider della risorsa chiede la provenienza dell'utente (WAYF)
- 2) L'utente sceglie il proprio IdP per l'autenticazione/autorizzazione
- 3) L'IdP utente comunica al SP l'avvenuta autenticazione e invia gli attributi per l'autorizzazione
- 4) Se gli attributi sono quelli richiesti dall'applicazione l'utente viene autorizzato all'utilizzo.



1) Accesso ad un Servizio IDEM

Home **Faq** **Supporto** **Gruppo Netcast** **Il GARR**

Servizi

- Login

Informazioni

- E' la prima volta?
- Che cosa e' Vconf
- Come funziona
- Requisiti tecnici
- Tutorial
- Documentazione
- Approfondimenti
- Banner e loghi

Login

Username (EMAIL):

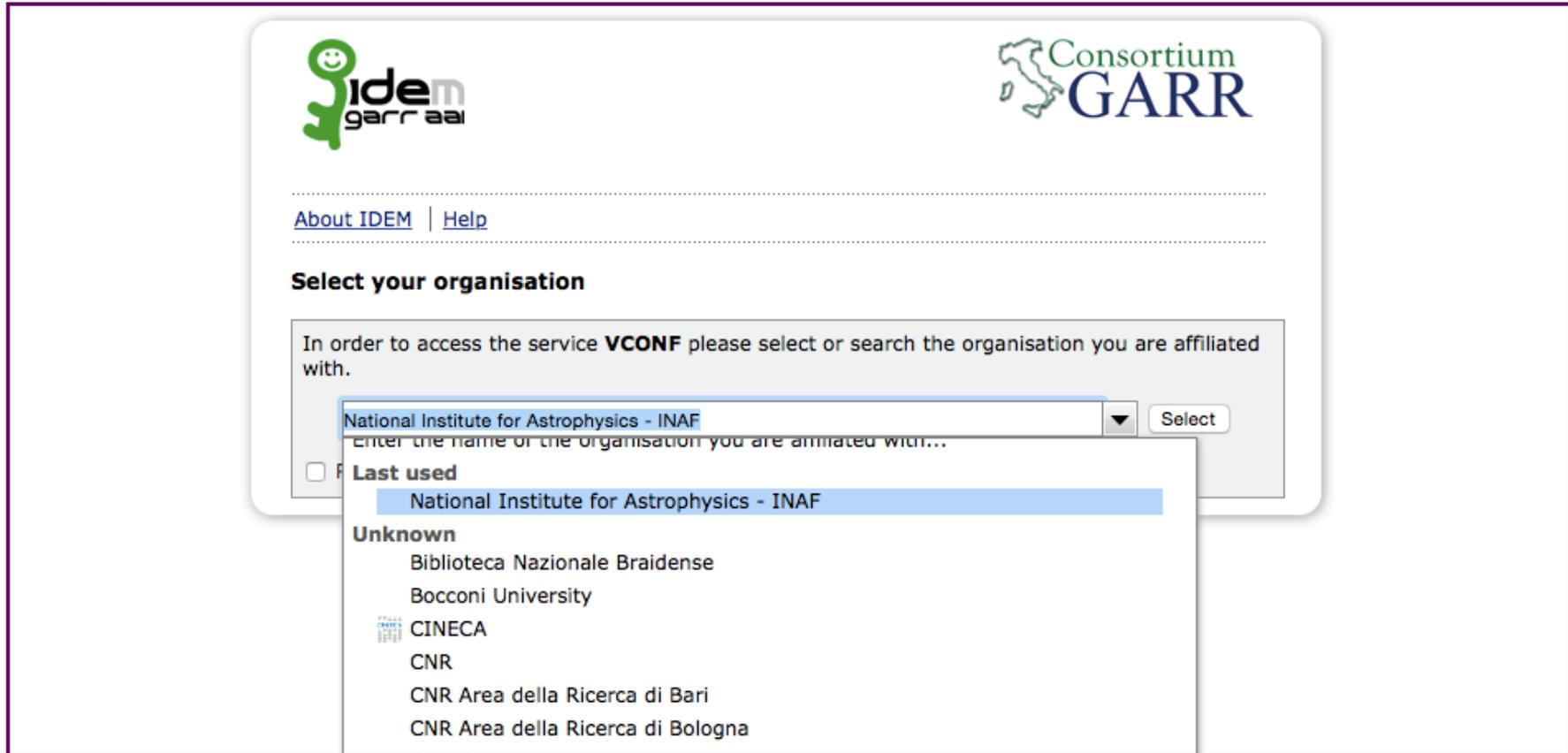
Password: non ricordi la password? Clicca [qui](#)

[istruzioni per il primo accesso](#)

Se sei registrato con IDEM clicca [qui](#)

In caso di problemi con il login attraverso IDEM clicca [qui](#)

2) IDEM Where Are You From



The screenshot shows the IDEM web interface. At the top left is the 'Idem garr aai' logo. At the top right is the 'Consortium GARR' logo, which includes a map of Italy. Below the logos are two links: 'About IDEM' and 'Help'. The main heading is 'Select your organisation'. Below this is a text box with the instruction: 'In order to access the service **VCONF** please select or search the organisation you are affiliated with.' There is a search input field containing 'National Institute for Astrophysics - INAF' and a 'Select' button. A dropdown menu is open, showing a list of organizations. The first item is 'National Institute for Astrophysics - INAF', which is highlighted. Below it are 'Unknown', 'Biblioteca Nazionale Braidense', 'Bocconi University', 'CINECA', 'CNR', 'CNR Area della Ricerca di Bari', and 'CNR Area della Ricerca di Bologna'.

Idem garr aai

Consortium GARR

[About IDEM](#) | [Help](#)

Select your organisation

In order to access the service **VCONF** please select or search the organisation you are affiliated with.

National Institute for Astrophysics - INAF

Enter the name of the organisation you are affiliated with...

Last used

- National Institute for Astrophysics - INAF

Unknown

- Biblioteca Nazionale Braidense
- Bocconi University
-  CINECA
- CNR
- CNR Area della Ricerca di Bari
- CNR Area della Ricerca di Bologna

3) Autenticazione al proprio IdP

INAF ISTITUTO NAZIONALE DI ASTROFISICA
NATIONAL INSTITUTE FOR ASTROPHYSICS

Idem garr aai

ACCESSO AL SERVIZIO RICHIESTO

L'Istituto Nazionale di Astrofisica (INAF) partecipa a IDEM (IDeNtity Management federato per l'accesso ai servizi) per la realizzazione dell'infrastruttura di Autenticazione e Autorizzazione federata della rete GARR.

Le credenziali di accesso vengono rilasciate a tutti i dipendenti e gli afferenti alle strutture INAF a livello nazionale. Per accedere al servizio richiesto inserisci le tue credenziali:

Vconf is the multivideoconference service offered by GARR that allows to activate one or more virtual meeting rooms

Username:

Password:

Per informazioni o assistenza scrivete a inaf-idem@ced.inaf.it

EDU GAIN

- IDEM INFO
- IDEM HOME
- RISORSE ATTIVE
- IDEM FAQS
- EDUGAIN
- IDP INFO**
- IDP HOME
- CREDENZIALI INAF
- PRIVACY

IDP CNR – Amministrazione Centrale

Username:

Password:

Supporto per gli utenti

4) Utilizzo del Servizio

Dopo l'Autenticazione e l'invio degli attributi di Autorizzazione si ritorna al servizio per utilizzarne le potenzialità.

Benvenuto **Franco Tinarelli** | [Logout](#)

■ Home ■ Faq ■ Supporto ■ Gruppo Netcast ■ Il GARR

Conferenze programmate

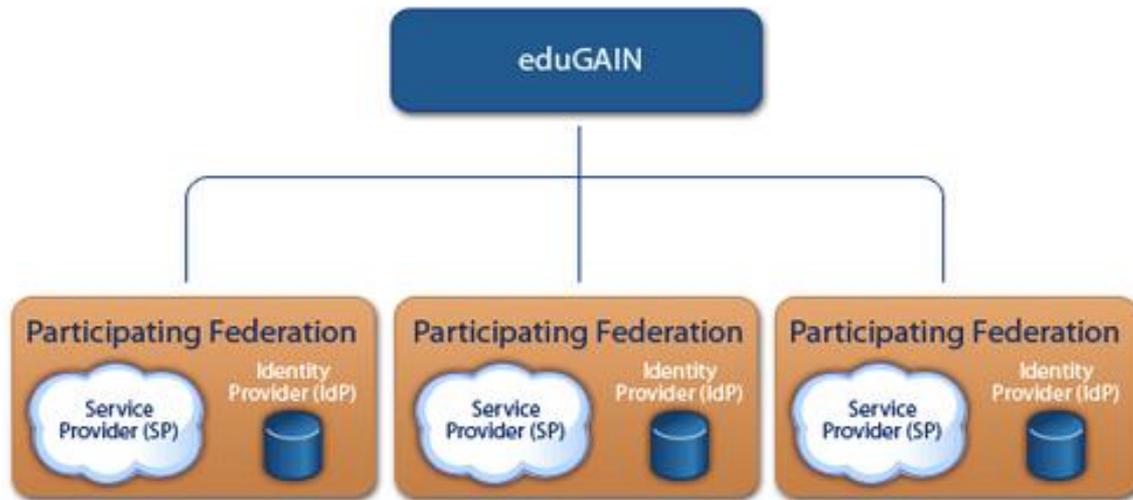
Non vi sono conferenze attualmente prenotate. [Crea una nuova prenotazione.](#)

Servizi

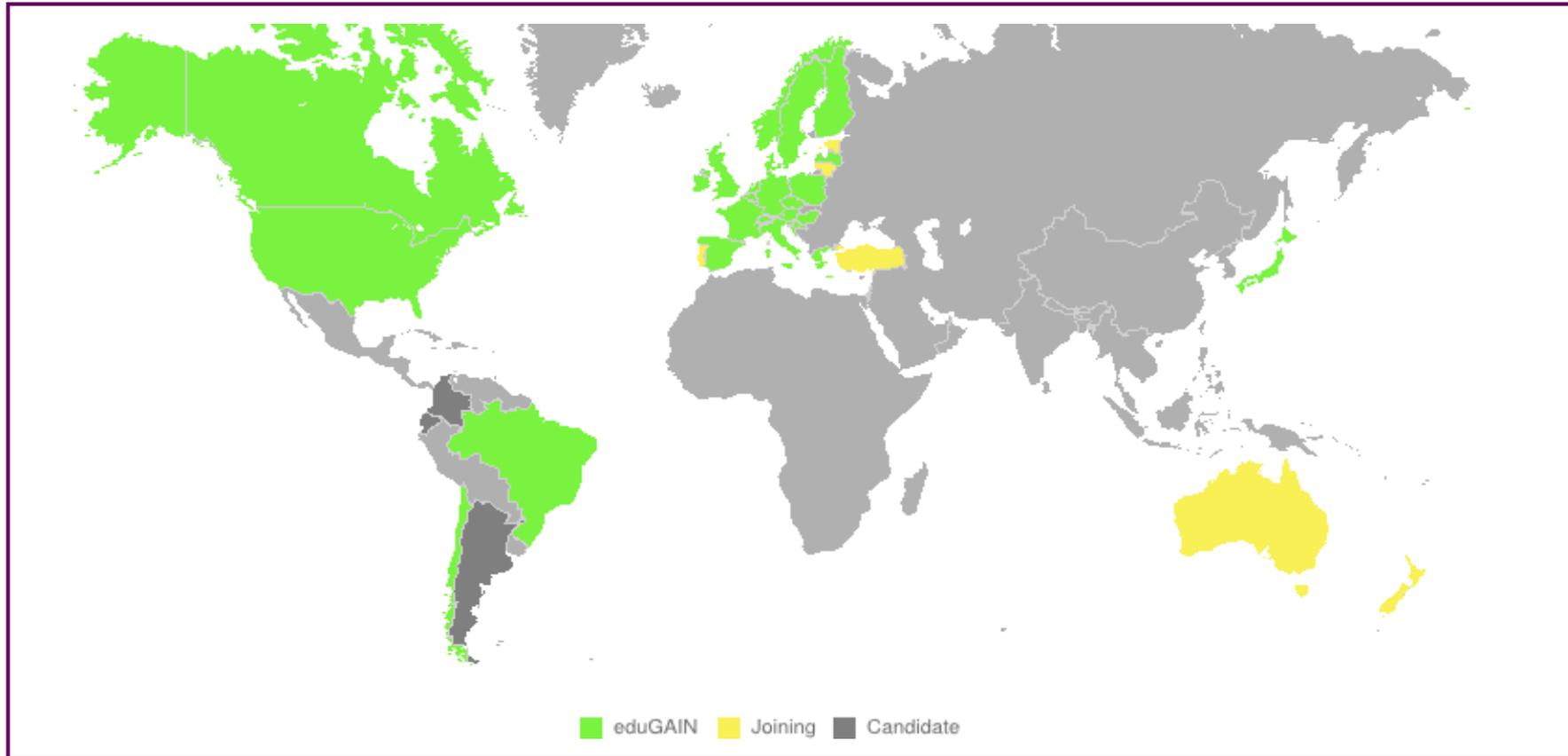
- ▶ Videoconferenza HD
- ▶ Videoconferenza SD
 - [Le mie prenotazioni SD](#)
 - [Nuova Prenotazione SD](#)
- ▶ Gestione Utenti

- **VCONF** per prenotare multi conferenze utilizzando la MCU del GARR
<https://vconf.garr.it>
- **FILESENDER** per inviare files di grosse dimensioni <https://filesender.garr.it>
- **Terena e-Science** certificato personale valido per l'utilizzo di servizi GRID
- **Terena Personal** certificato personale
- Sono in preparazione nuovi servizi interessanti:
 - **GARRbox** (la Cloud del GARR)
 - **WebMeeting** (la possibilita' di creare stanze web per meeting e seminari)
 - **WebEx** (la possibilità di creare stanze per meeting web e collegarle alla MCU GARR)
- **WI-FI** in molte Università, al comune di Trieste e Udine, sono già attivi accessi Wireless con login IDEM.

IDEM, da Ottobre 2011, ha aderito ad eduGAIN, l'interfederazione che interconnette le Federazioni di identità e permette agli utenti di accedere ai servizi in rete tramite un sistema di SSO su scala internazionale usando l'unica password data dalla propria Organizzazione di appartenenza. eduGAIN è un servizio sviluppato all'interno del progetto GÉANT. (<http://www.edugain.org>)



Le Federazioni in eduGAIN



- Per scoprire quali servizi le Federazioni partecipanti mettono a disposizione si può consultare la pagina web: <http://www.edugain.org/technical/status.php> contiene l'elenco dei link alle pagine web delle varie Federazioni, dalle quali è possibile risalire agli elenchi dei servizi di ogni federazione.
- La federazione Greca, con fondi della Comunità Europea, ha creato un interessante servizio di Cloud Computing chiamato **~okeanos** che la comunità scientifica partecipante ad eduGAIN può utilizzare gratuitamente.
- Per accedere ad **~okeanos** bisogna registrarsi utilizzando le credenziali della propria Federazione al link <https://okeanos-global.grnet.gr/home/>. Dopo la registrazione l'accesso avverrà sempre con le credenziali del proprio IdP.

okeanos GLOBAL

[About](#)
[Services](#)
[Resources](#)
[OpenSource](#)
[Support](#)

[create an account now >](#)



WELCOME TO OKEANOS GLOBAL!

This is GRNET's cloud service, for the GÉANT Research and Academic Community. With ~okeanos global you are one click away from your own Virtual Machines, Networks and Storage.

STATISTICS

Spawned VMs	Active VMs	Spawned Networks
32,430	368	11,254

oceanos GLOBAL



SIGN UP

Sign in

Choose one of the following sign up methods.

ACADEMIC



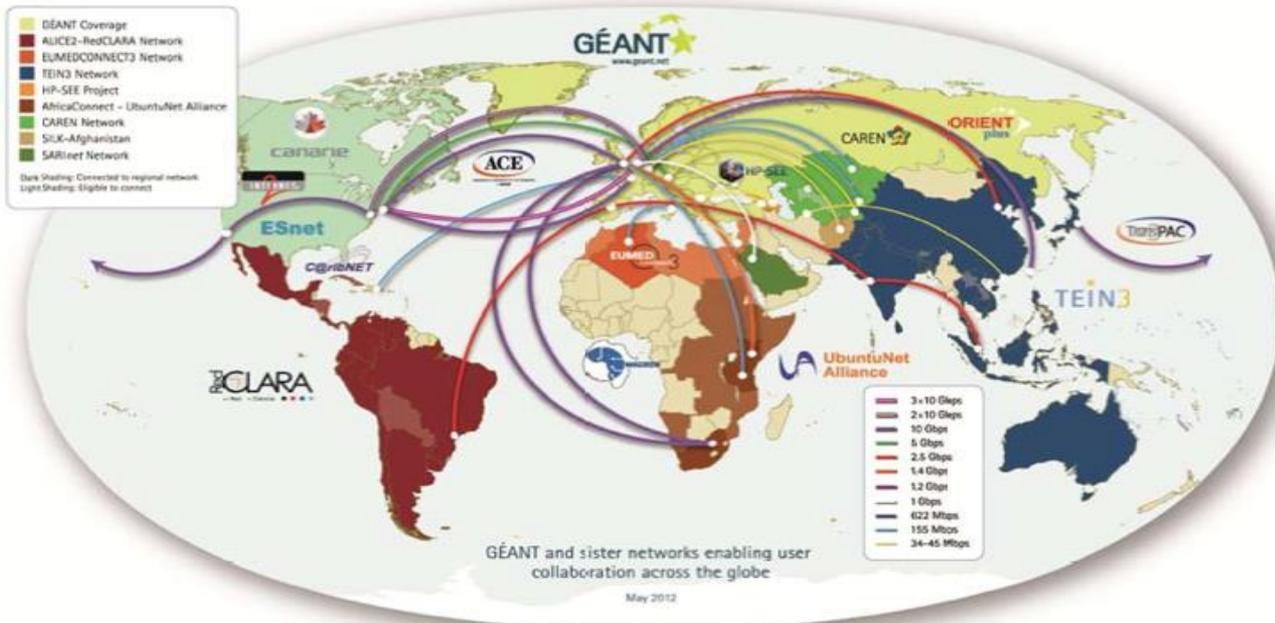
AAI

GRNET Federation
Authentication & Authorization Infrastructure

Select your country
to filter available providers

CSP - innovation in ICT 🇮🇹 Italy 219 km	
Scuola Superiore Sant'Anna 🇮🇹 Italy 221 km	
National Institute for Astrophysics - INAF 🇮🇹 Italy 245 km	
Università di Napoli Parthenope	

GÉANT At the Heart of Global Research Networking



GÉANT and sister networks enabling user collaboration across the globe

May 2012

- **eduroam (Education Roaming)** è un servizio che offre un accesso wireless sicuro alla rete. Gli utenti roaming che visitano un istituto che aderisce all'iniziativa sono in grado di utilizzare la rete locale wireless (WLAN) usando le stesse credenziali (username e password) che userebbero nella propria istituzione d'appartenenza, senza la necessità di ulteriori formalità presso l'istituto ospitante.
- eduroam è un'infrastruttura basata su una rete di server RADIUS che utilizza 802.1x
- Lo scopo della Federazione Italiana eduroam è di facilitare l'accesso alla rete GARR e alle altre reti ad essa connesse, agli utenti (roaming users) delle organizzazioni partecipanti (servizio eduroam).
- La Federazione è coordinata dal Consortium GARR, che la rappresenta presso le altre federazioni e confederazioni. eduroam è un marchio registrato di TERENA

eduroam nel mondo



- INAF ha registrato il realm **inaf.it** e il CNR il realm **cnr.it** gli Enti gestiscono i server Radius per l'autenticazione.
- Il server Radius delega l'autenticazione al server LDAP dell'Ente permettendo l'utilizzo delle stesse credenziali sia per eduroam sia per IDEM.
- eduroam usa una Username composta dal nome utente e dal realm es. cognome.nome@inaf.it / nome.cognome@cnr.it
- Le sedi che attivano il servizio dovrebbero fornirsi di access point wireless multi SSID per fornire l'accesso ad eduroam con SSID eduroam
- Al link <http://www.ced.inaf.it/serv/index.php/servizi/wifi-eduroam> trovate gli esempi di configurazione per i portatili.



I flussi di A&A

