



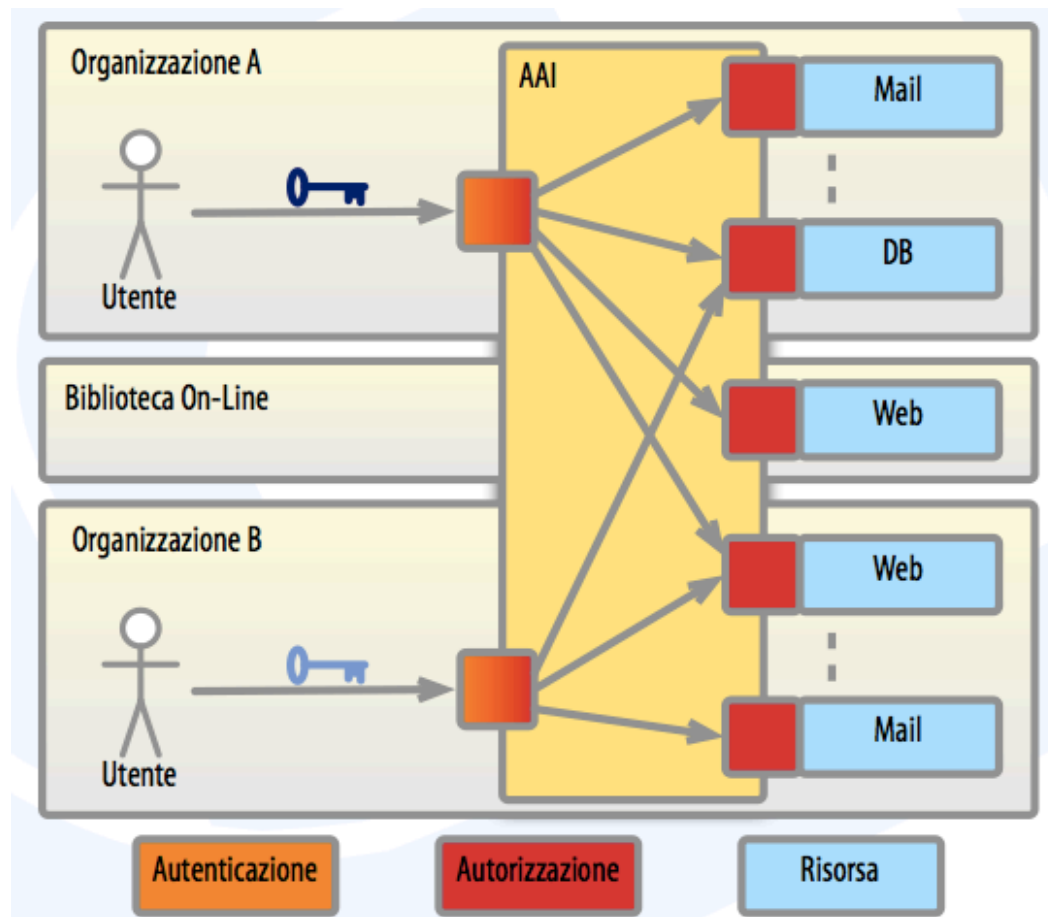
IDEM eduroam

Infrastrutture di Autenticazione e Autorizzazione
(Franco Tinarelli - Coffee talk - IRA 13 aprile 2012)

IDEM (IDEntity Management)

- **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



IdP (Identity Provider)

- 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.
- INAF partecipa 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.

SP (Service Provider)

-
- L'accesso al servizio attiva la catena di Autenticazione/ Autorizzazione
- Il servizio viene fornito solo ricevendo tutti gli attributi richiesti

GARR VCONF



GARR/CINECA

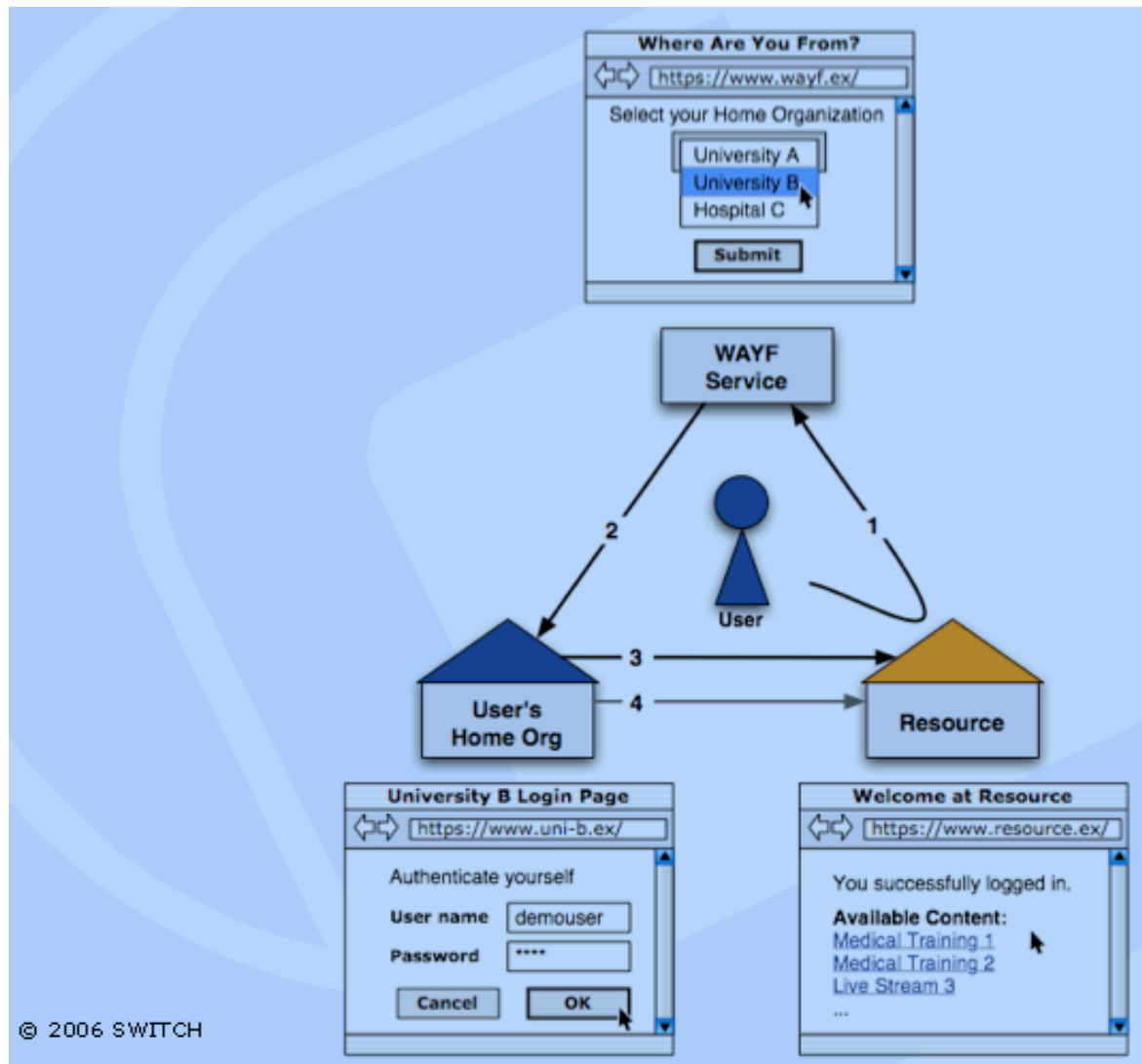


ePTID (R), ePSA (R), sn (R),
givenName (R), mail (R)

IDEM e Shibboleth

- Shibboleth è un progetto del gruppo [Internet2](#) che si prefigge di sviluppare una soluzione open source per l'accesso a risorse/servizi web condivisi tramite credenziali di autorizzazione, e' compatibile con SAML.
- SAML è un framework basato su XML per comunicare, tra un authority e terze parti fidate, l'avvenuta autenticazione dell'utente, il suo aver diritto ad usufruire di una risorsa/servizio e i suoi attributi. Il suo acromino è SAML. Shibboleth supporta diversi formati, protocolli e versioni di SAML

Lo schema di AA con Shibboleth



IDEM: le Credenziali INAF

- 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 INAF”
- Le credenziali sono gestite dai server del Centro Elaborazione Dati Amministrativi dell'INAF ed utilizzate dall'IdP (Identity Provider) dell'INAF.

INAF - IDEM Info - Mozilla Firefox

Firefox INAF - IDEM Info

inaf.it https://www.ced.inaf.it/idem-info/ Google



INAF ISTITUTO NAZIONALE DI ASTROFISICA
NATIONAL INSTITUTE FOR ASTROPHYSICS



Idem
garr aai

IDEM INFO

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



Shibboleth.

PARTECIPAZIONE A IDEM

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. Le modalita` di rilascio, utilizzo e revoca delle credenziali sono contenute nel Documento descrittivo del processo di accreditamento degli utenti dell'INAF (DOPAU in formato [PDF](#))

ASSISTENZA PER GLI UTENTI


inaf-idem@ced.inaf.it

REFERENTE TECNICO PER L'IDP

Franco Tinarelli
f.tinarelli@ira.inaf.it
+39 051 6399409

- Il nome utente (username o User ID) utilizzato per l'autenticazione ai servizi IDEM, e` costituito dalla sequenza del cognome e nome in minuscolo separati da un (.) punto (es. rossi.mario). La sequenza Cognome e Nome rispetta le regole sulle omonimie e troncature utilizzate per i cedolini web.
- La parola chiave (password:) utilizzata dall'IdP e' bloccata per tutti gli utenti che non hanno ancora utilizzato i servizi IDEM, per sbloccarla e impostarla dovete utilizzare la voce "GESTIONE PASSWORD" del menu.

RISORSE ATTIVE	Le credenziali sono gestite dai server del Centro Elaborazione Dati Amministrativi dell'INAF ed utilizzate dall'IdP (Identity Provider) dell'INAF. Il nome utente (username o User ID) utilizzato per l'autenticazione ai servizi IDEM, e` costituito dalla sequenza del cognome e nome in minuscolo separati da un (.) punto (es. rossi.mario). La sequenza Cognome e Nome rispetta le regole sulle omonimie e troncature utilizzate per i cedolini web. La parola chiave (password:) utilizzata dall'IdP e' bloccata per tutti gli utenti che non hanno ancora utilizzato i servizi IDEM, per sbloccarla e impostarla dovete utilizzare la voce "GESTIONE PASSWORD" del menu.
IDEM FAQS	
IDP INFO	
IDP HOME	
PRIVACY	
GESTIONE PASSWORD	



- Non avendo mai impostato la password, come prima operazione dovete seguire il link “password reset” che vi permetterà di assegnarvi una password temporanea generata automaticamente.

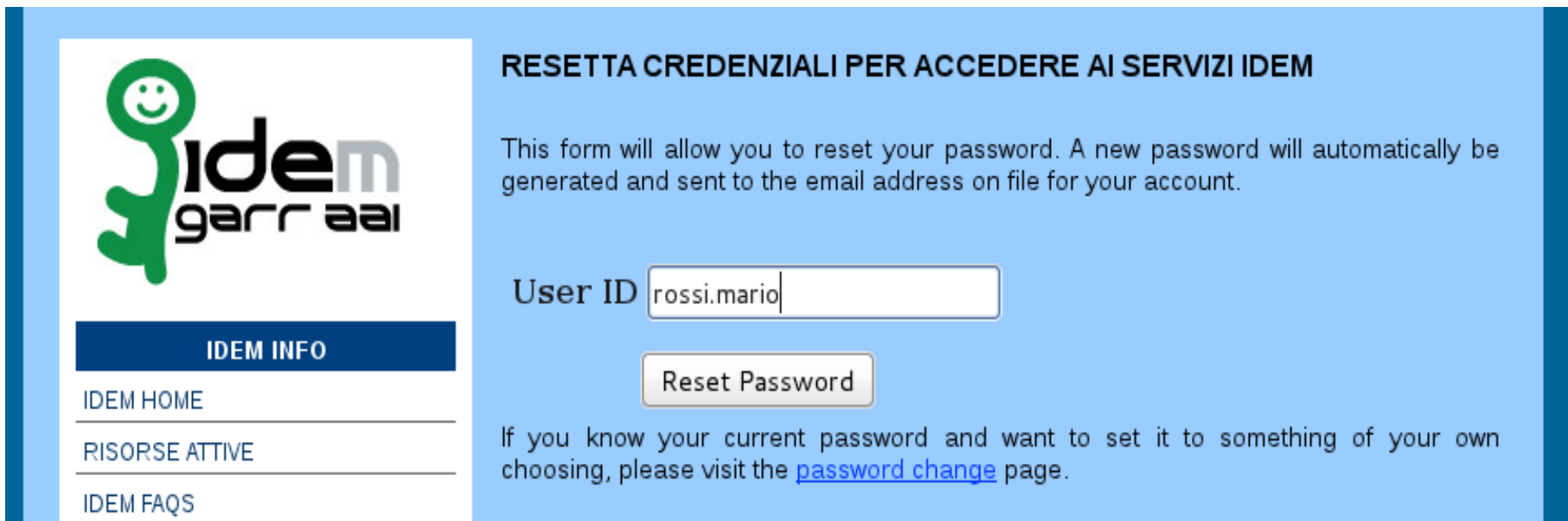


ATTIVAZIONE CREDENZIALI PER ACCEDERE AI SERVIZI IDEM

Se non hai ancora attivato le tue credenziali o non ricordi la vecchia password devi prima visitare la pagina di [password reset](#).

MODIFICA CREDENZIALI PER ACCEDERE AI SERVIZI IDEM

- Inserite il vostro cognome e nome rispettando la sintassi riportata nell'esempio e premete il pulsante “Reset Password”. Vi ricordo che il vostro cognome e il vostro nome sono gli stessi che utilizzate per l'accesso alla pagina web che vi permette di scaricare o consultare i cedolini degli stipendi.



The screenshot shows a web interface for resetting a password. On the left is a sidebar with the IDEM logo (a green stick figure) and the text 'idem garr aai'. Below the logo are navigation links: 'IDEM INFO' (highlighted), 'IDEM HOME', 'RISORSE ATTIVE', and 'IDEM FAQS'. The main content area has a blue background and is titled 'RESETTA CREDENZIALI PER ACCEDERE AI SERVIZI IDEM'. It contains an explanatory paragraph, a text input field for 'User ID' with the example 'rossi.mario', a 'Reset Password' button, and a final paragraph with a link to the 'password change' page.

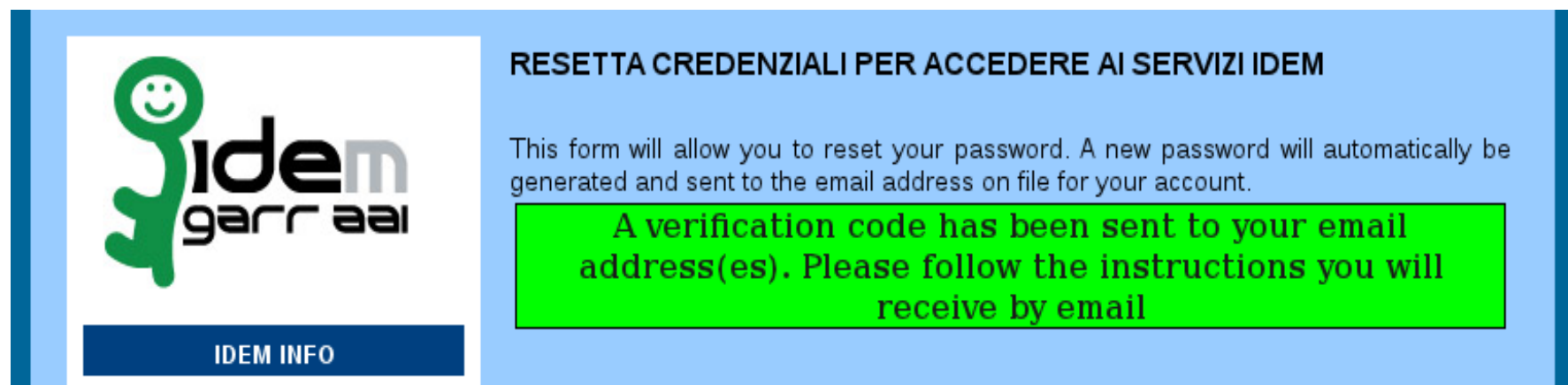
RESETTA CREDENZIALI PER ACCEDERE AI SERVIZI IDEM

This form will allow you to reset your password. A new password will automatically be generated and sent to the email address on file for your account.

User ID

If you know your current password and want to set it to something of your own choosing, please visit the [password change](#) page.

- Questa operazione invierà al vostro indirizzo di posta elettronica una prima mail contenente la richiesta di conferma di impostazione/modifica password, questo serve ad accertare che la richiesta sia effettivamente partita da voi.



The screenshot shows a confirmation page for resetting IDEM credentials. On the left, there is a logo for 'idem garr aai' featuring a green stick figure with a smiley face. Below the logo is a dark blue button labeled 'IDEM INFO'. The main content area has a light blue background. At the top, it says 'RESETTA CREDENZIALI PER ACCEDERE AI SERVIZI IDEM'. Below that, a paragraph explains that the form allows password resets and that a new password will be sent to the user's email. A prominent green box with black text states: 'A verification code has been sent to your email address(es). Please follow the instructions you will receive by email'.

idem garr aai

IDEM INFO

RESETTA CREDENZIALI PER ACCEDERE AI SERVIZI IDEM

This form will allow you to reset your password. A new password will automatically be generated and sent to the email address on file for your account.

A verification code has been sent to your email address(es). Please follow the instructions you will receive by email

- Il testo della mail, come da esempio riportato, contiene il link da seguire per impostare la password temporanea che vi sarà inviata in una seconda mail:

To: mario.rossi@inaf.it
Subject: Password Reset
From: ced-staff@ced.inaf.it
Reply-To: no_ced-staff@ced.inaf.it
Message-Id: <20120113105012.31FE569249@netserver.ced.inaf.it>
Date: Fri, 13 Jan 2012 11:50:12 +0100 (CET)

A request has been made to reset your password.

To activate your password reset, click on the following link:

<https://www.ced.inaf.it/passwd/verify.php?act=1508c23f755d56d30819dc7845148a62f07f0401>

(you may need to cut and paste the link into your web browser)

If you did not request the password reset, please reply to this message. Be sure to include the following information in your email:

Date: Fri Jan 13 11:50:12 CET 2012
Requesting IP: xxx.xxx.xxx.xxx



IDEM INFO

IDEM HOME

RESET CREDENZIALI PER ACCEDERE AI SERVIZI IDEM

This form will allow you to reset your password. A new password will automatically be generated and sent to the email address on file for your account.

Your password has been successfully changed and sent to your email address(es) on file

If you know your current password and want to set it to something of your own choosing, please visit the [password change](#) page.

From: ced-staff@ced.inaf.it

Reply-To: no_ced-staff@ced.inaf.it

Message-Id: <20120113105447.9A41669249@netserver.ced.inaf.it>

Date: Fri, 13 Jan 2012 11:54:47 +0100 (CET)

A request has been made to reset your password. Your new password is as follows:

JC6BX7

It is recommended that you change your password to something that you can remember as soon as possible.

...

- A questo punto potete ritornare sulla pagina web di modifica delle password e impostare la vostra password definitiva.

INAF IDP - Cambio Credenziali - Mozilla Firefox

Firefox INAF IDP - Cambio Credenziali INAF IDP - Cambio Credenziali

inaf.it https://www.ced.inaf.it/passwd/ Google

INAF ISTITUTO NAZIONALE DI ASTROFISICA
NATIONAL INSTITUTE FOR ASTROPHYSICS

Idem
garr aai

IDEM INFO

IDEM HOME

RISORSE ATTIVE

IDEM FAQs

IDP INFO

IDP HOME

CREDENZIALI INAF

PRIVACY

Shibboleth.

ATTIVAZIONE CREDENZIALI PER ACCEDERE AI SERVIZI IDEM

Se non hai ancora attivato le tue credenziali o non ricordi la vecchia password devi prima visitare la pagina di [password reset](#).

MODIFICA CREDENZIALI PER ACCEDERE AI SERVIZI IDEM

Questa form ti permette di cambiare la tua password. Ti preghiamo di scegliere una nuova password conforme alle caratteristiche di sicurezza richieste.

Change Form

User ID

Current Password

New Password

New Password (again)

Change Password

INAF e le Credenziali IDEM

- Con le credenziali IDEM e' ora possibile accedere a tutti i servizi che la federazione offre:

<https://www.idem.garr.it/index.php/en/services/sp>

- tra questi quello che vi permettera' di prenotare le vostre multi conferenze utilizzando la MCU del GARR: il servizio si chiama Vconf ed e' raggiungibile alla URL

<https://vconf.garr.it>

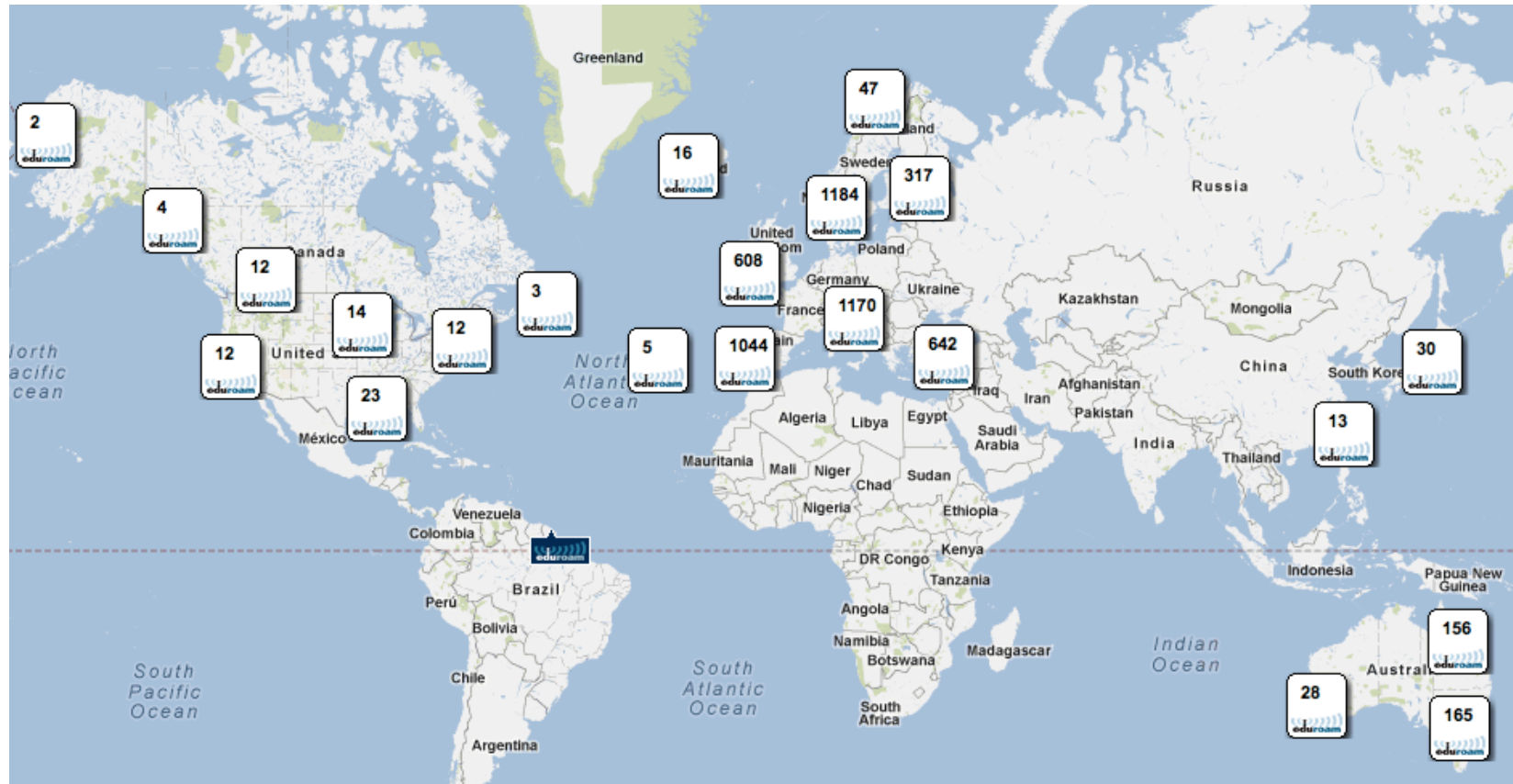
- oppure quello per inviare ai vostri corrispondenti files di grosse dimensioni: il servizio si chiama GARR Filesender

<https://filesender.garr.it>

eduroam

- **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 mobili (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



eduroam e INAF

- INAF ha registrato il realm inaf.it e gestisce il 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](#)
- IRA e' fornita di access point wireless multi SSID e fornisce l'accesso ad eduroam con SSID eduroam
- Al link http://www.ced.inaf.it/serv/index.php?option=com_content&view=article&id=185&Itemid=189 trovate gli esempi di configurazione per I portatili.

Link utili

- www.idem.garr.it
- <http://vconf.garr.it>
- www.servizi.garr.it/index.php/it/eduroam
- www.eduroam.org
- www.ced.inaf.it/idem-info
- http://www.ced.inaf.it/serv/index.php?option=com_content&view=article&id=184&Itemid=120

INAF in IDEM/eduroam per colpa di chi...

- Barbara Neri, Stefano Giovannini (CED/IRA)
- Giuliano Taffoni (IASF-BO)
- Franco Tinarelli, Marco Tugnoli, Mauro Nanni, Simona Tubertini (IRA/AdR BO)