



Franco Tinarelli
INAF – IRA

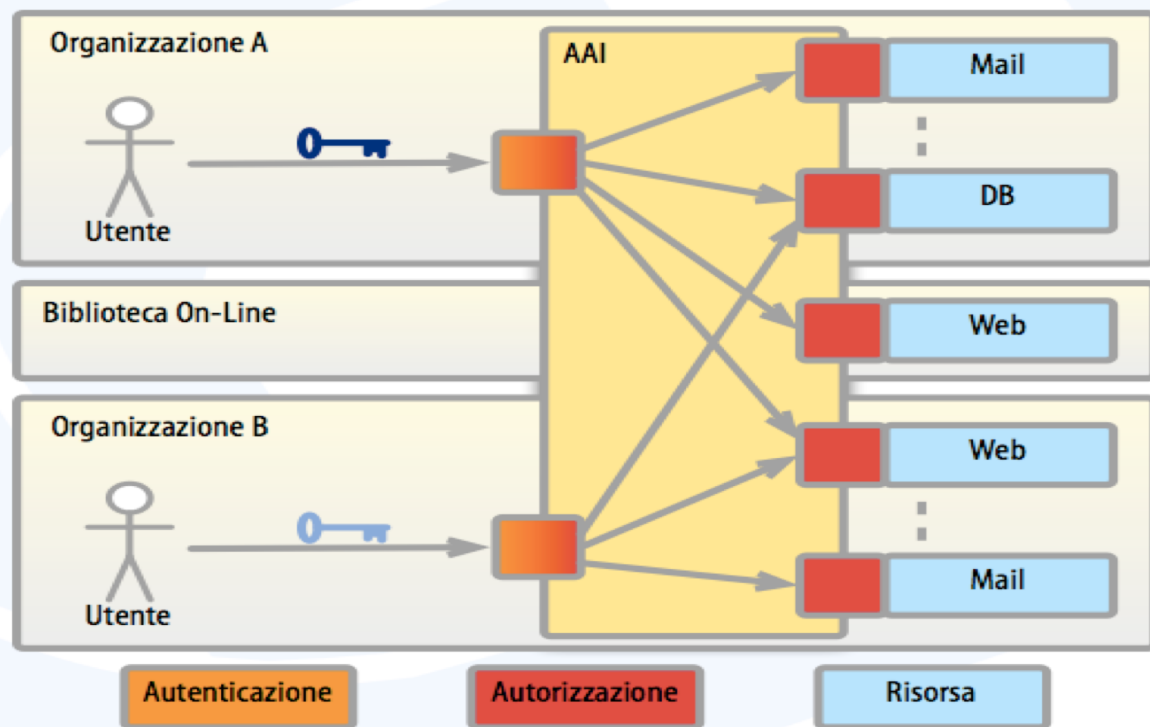
Pula – Cagliari
16 – 19/09/2014

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

IDEM (Identity Management)

- Uniche Credenziali per piu' Servizi Federati



IDEM 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.

IDEM SP (Service Provider)

- 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

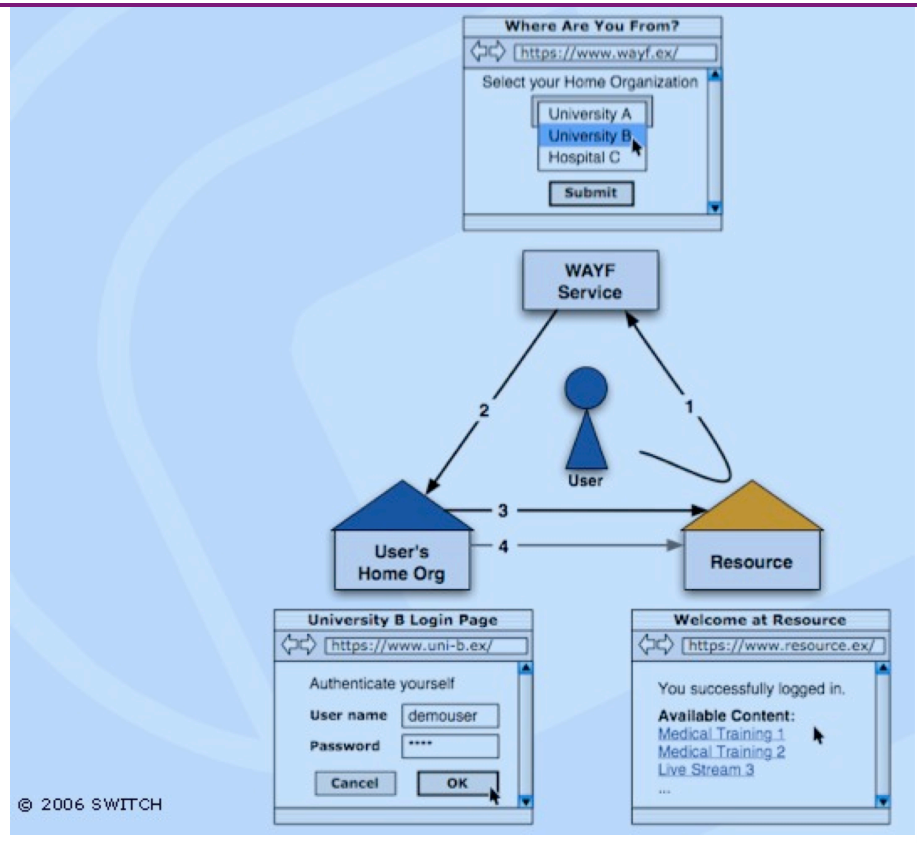


ePTID (R), ePSA (R), sn (R),
givenName (R), mail (R)

- Shibboleth è un progetto del gruppo Internet2 (ora è un consorzio soprattutto europeo) 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 (Security Assertion Markup Language).
- SAML è un framework basato su XML per comunicare, tra una authority e terze parti fidate, l'avvenuta autenticazione dell'utente, il suo aver diritto ad usufruire di una risorsa e i suoi attributi. Shibboleth supporta diversi formati, protocolli e versioni di SAML. (la versione corrente OpenSAML 2.6.2)

Lo schema di A&A con Shibboleth

- 1) L'utente accede alla risorsa web, il service provider della risorsa chiede la provenienza dell'utente (WAIF)
- 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.



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

IDEM (Credenziali degli Utenti)



IDEM INFO

[IDEM HOME](#)

[RISORSE ATTIVE](#)

[IDEM FAQs](#)

IDP INFO

[CREDENZIALI DEGLI UTENTI](#)

[PRIVACY](#)

[GESTIONE PASSWORD](#)



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 modalità 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

IDEM (Credenziali degli Utenti)

- 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.



del 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.

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

IDEM (Credenziali degli Utenti)

- 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.

password reset.' A red arrow points from this text to the 'password reset' link. The bottom section is titled 'MODIFICA CREDENZIALI PER ACCEDERE AI SERVIZI IDEM' and contains the text: 'Questa form ti permette di cambiare la tua password. Ti preghiamo di scegliere una nuova password conforme alle caratteristiche di sicurezza richieste.'" data-bbox="47 469 938 867"/>

ATTIVAZIONE CREDENZIALI PER ACCEDERE AI SERVIZI IDEM

Se non hai ancora attivato le tue credenziali (**cognome.nome**) 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.

IDEM (Credenziali degli Utenti)

- Inserite il vostro cognome e nome rispettando la sintassi riportata nell'esempio (**rossi.mario**) 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.



IDEM INFO

IDEM HOME

RISORSE ATTIVE

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.

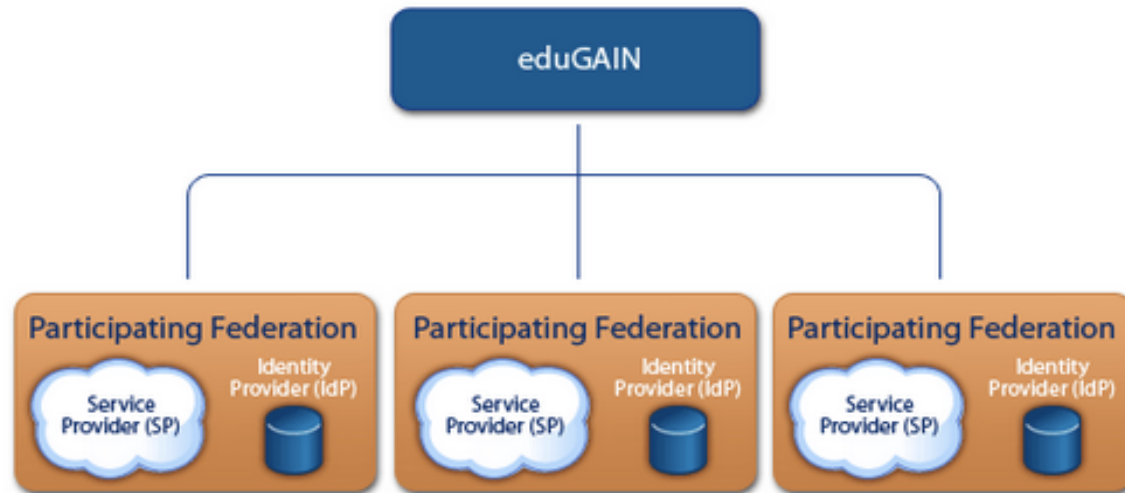
IDEM (Credenziali degli Utenti)

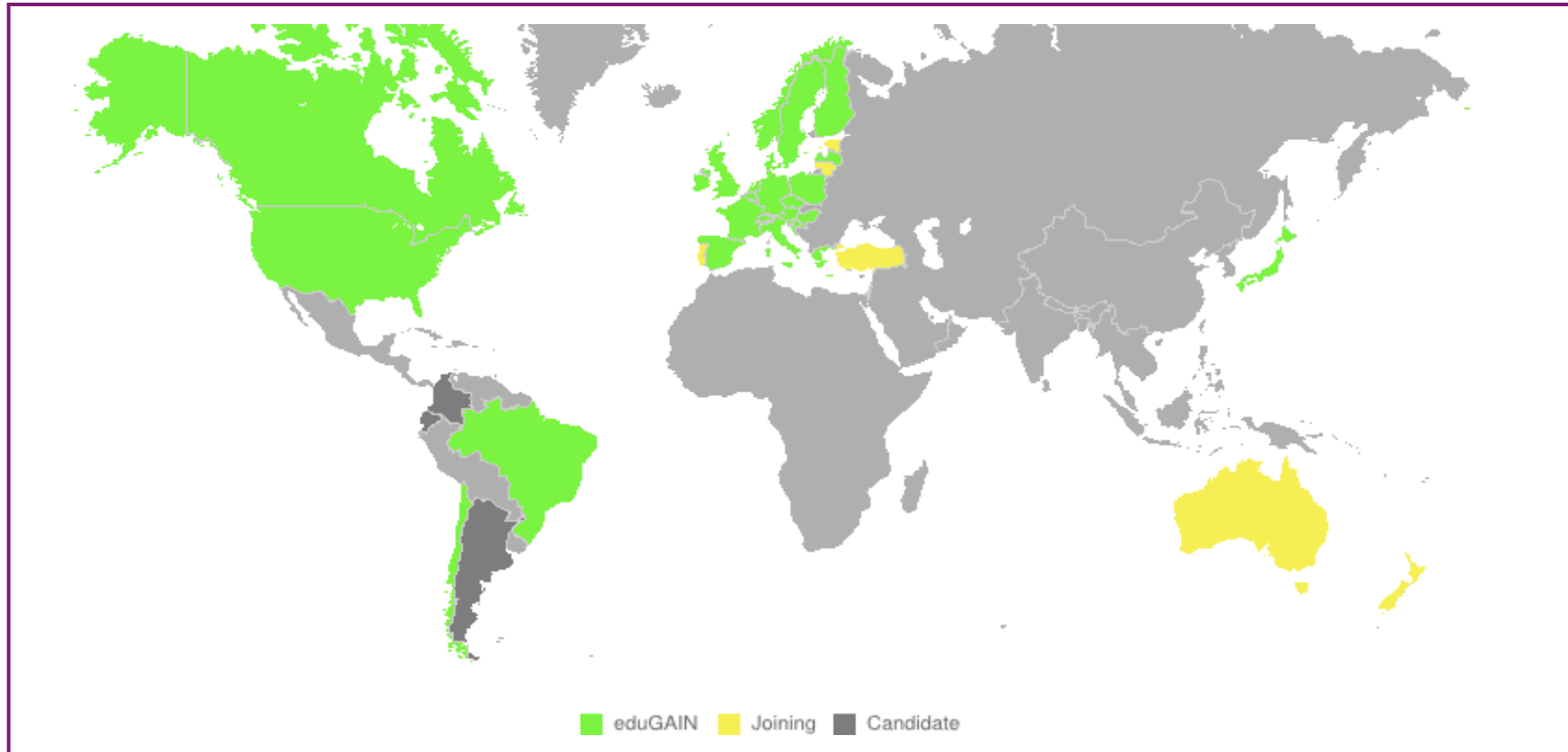
- Questa operazione invierà al vostro indirizzo di posta elettronica una **prima mail** contenente la richiesta **di conferma** di impostazione/modifica password, questo serve ad accertare che la richiesta sia effettivamente partita da voi.
- Il testo della mail contiene il link da seguire per **ricevere** la **password temporanea** che vi sarà inviata in una **seconda mail**.
- A questo punto potete ritornare sulla pagina web di modifica delle password e impostare la vostra **password definitiva** nelle form di input della sezione **“Change Form”**.

IDEM (Credenziali degli Utenti)

- 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>
- Terena rilascia certificati utente Personal ed e-Science
- 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)
- In molte Università 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>)





Il GARR organizza un corso per chi ha l'esigenza di abilitare applicazioni web all'autenticazione federata utilizzando SAML. Informazioni e Iscrizioni <http://idem.garr.it>

Abilitare le applicazioni web al Single Sign-on con strumenti SAML

30 Settembre 2014

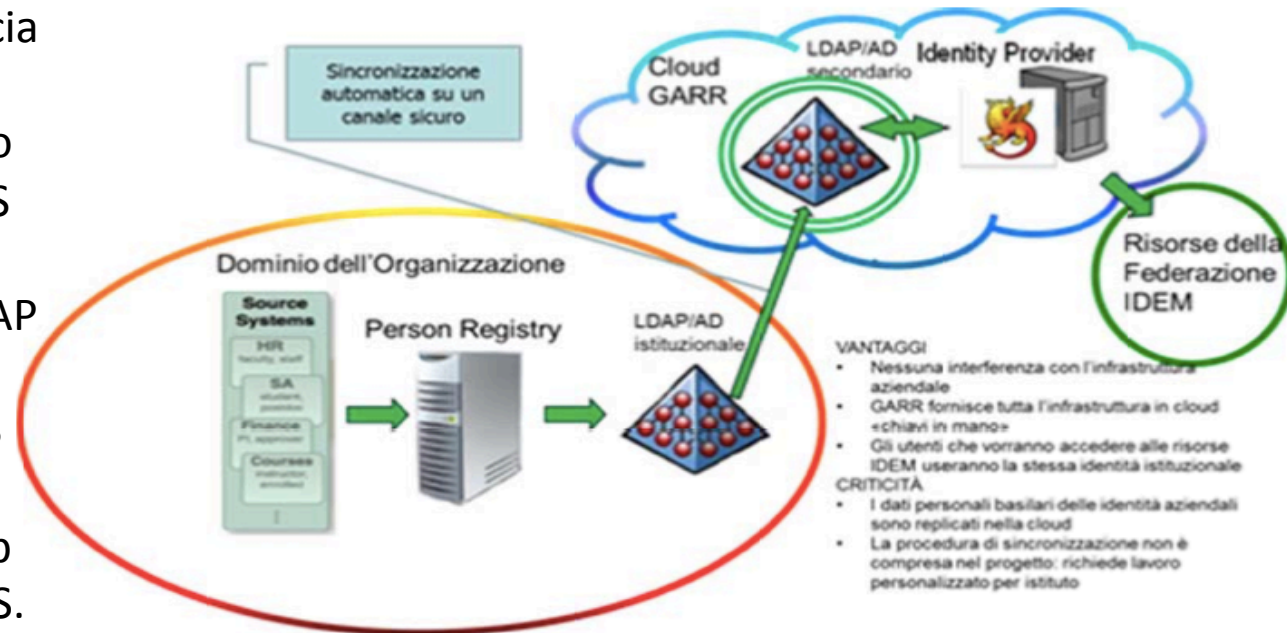
Consortium GARR, Roma



- Con il Progetto GARR-X Progress il GARR realizzerà una rete telematica di nuova generazione completamente in fibra ottica, integrata con l'infrastruttura nazionale GARR-X e le reti della ricerca europee e mondiali, nelle 4 Regioni della Convergenza (Puglia, Calabria, Sicilia, Campania). Su questa infrastruttura sarà possibile offrire servizi ad alto valore aggiunto, quali connettività fino a 10, 40 e 100Gbps e cammini ottici dedicati end-to-end, che permettano alle realtà di ricerca presenti nelle 4 Regioni di comunicare e trasmettere grandi quantità di dati ai partner in tutto il mondo, rendendo più efficienti le collaborazioni esistenti e facilitandone di nuove. Grazie al Progetto verrà realizzata una infrastruttura digitale integrata per il calcolo e l'archiviazione distribuita, che si appoggerà sulla nuova rete e offrirà alla comunità della ricerca e dell'istruzione sul territorio strumenti ICT.

GARR-X e Servizi IDP in Cloud

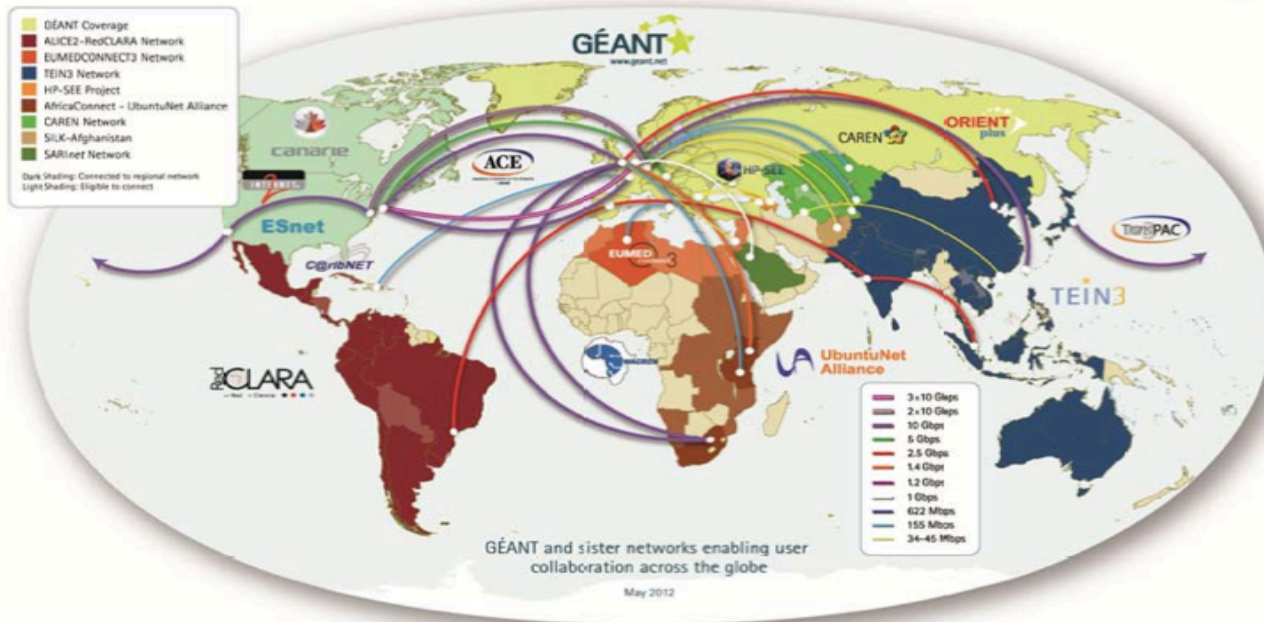
- 1) **Full:** IdP, LDAP server, interfaccia web per la gestione, fornito in modalità SaaS
- 2) **Replica:** IdP, LDAP server, in modalità PaaS
- 3) **Smart:** il solo IdP in modalità PaaS.



GARR-X Le Sedi INAF

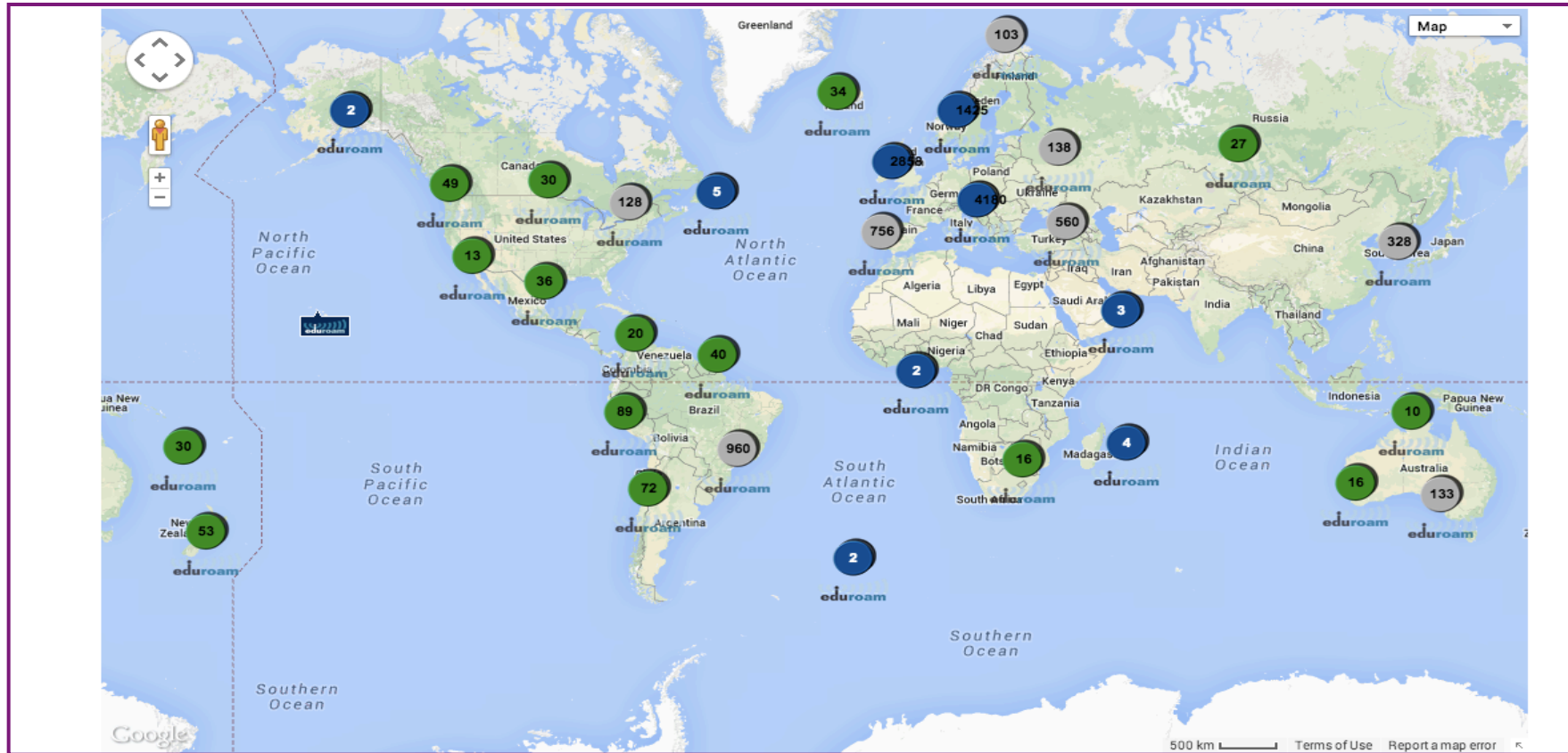
n.	Sede INAF	Indirizzo
1	INAF Osservatorio Astrofisico di Catania	Via S.Sofia, 70 – 95123 Catania
2	INAF Osservatorio Astronomico di Capodimonte	Salita Moiariello, 16 – 80131 Napoli
3	INAF Osservatorio Astronomico di Palermo	Piazza del Parlamento, 1 – 90134 Palermo
4	INAF-IASF - Palermo	Via Ugo La Malfa, 153 – 90146 Palermo
5	INAF laboratorio di Astrofisica Palermo	Via Gian Filippo Ingrassia, 31 - 90123 Palermo

GÉANT At the Heart of Global Research Networking



- **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 gestisce il server Radius per l'autenticazione. Il server Radius è installato presso il CED amministrativo di Bologna.
- 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](#)
- 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.

- Il server radius, presso l'istituto IRA, è collegato ai server GARR e offre il servizio di proxy per le sedi INAF che intendono attivare il servizio.
- Le sedi già attive sono:
 - Sede Centrale
 - IASF Milano
 - IASF Bologna
 - IRA Bologna
 - OA Trieste
 - OA Padova
 - OA Catania
 - IASF Palermo



I flussi di A&A

