Accesso ai dati astronomici e radioastronomici: Autenticazione e Autorizzazione in INAF.

Franco Tinarelli[1], Sonia Zorba[2], Cristina Knapic[2]

1 – INAF Istituto di Radioastronomia; 2 – INAF Osservatorio Astronomico di Trieste

franco.tinarelli@inaf.it sonia.zorba@inaf.it cristina.knapic@inaf.it

L'Istituto Nazionale di Astrofisica gestisce i dati prodotti dalle osservazioni di una serie di telescopi (Asiago, TNG e LBT) e radiotelescopi (Medicina, Noto e SRT). Essi vengono archiviati nei DB gestiti dal servizio IA2.

Per l'accesso ai dati è stata sviluppata una suite di applicazioni, in collaborazione tra IRA (Istituto di Radioastronomia) e IA2 (Archivi astronomici Italiani).

La suite è composta da un modulo di autenticazione chiamato RAP (Remote Authentication Portal) che permette l'autenticazione con EduGain, Google, Facebook, Linkedin , X.509 e con account registrati localmente.

La suite è completata da connettori per l'interazione con Grouper, un tool Java EE sviluppato da Internet2 per la gestione dei gruppi e delle identità.

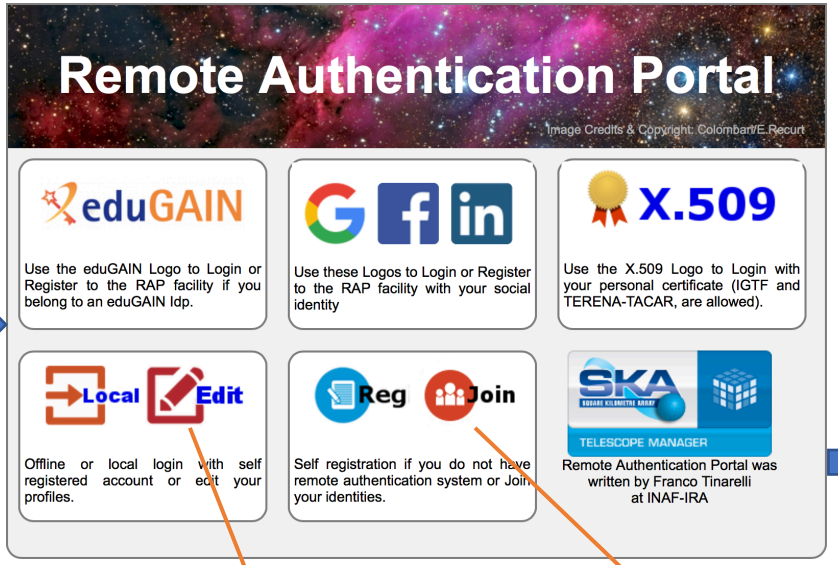
Grouper è stato scelto da IA2 per organizzare le autorizzazioni d'accesso alle risorse fornite tramite i propri servizi in quanto strumento maturo e già utilizzato con successo da altre organizzazioni che operano nell'ambito della ricerca. La suite RAP+Grouper è stata proposta come sistema di A&A per SKA.

I♥RAP RAP (Remote Authentication Portal)

RAP è stato sviluppato come prototipo A&A per SKA.

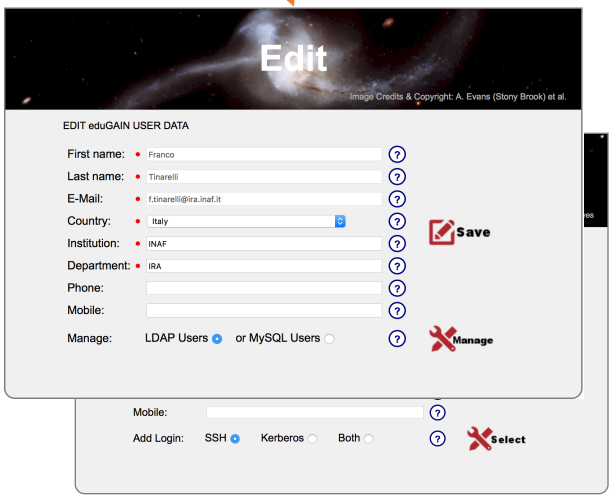
```
$SKA = array (
    'manager'  => "https://service_callback",
    'secret'   => "service secret",
    'client'   => "client ID",
    'logo'     => "TMlogo-200.png",
    'gui'      => "/rap/portal/RAP.php",
    'edugain'  => true,
    'google'   => true,
    'facebook' => true,
    'linkedin' => true,
    'x509'     => true,
    'local'    => true,
    'edit'     => true,
    'register' => true,
    'join'     => true,
    'use_dbms' => false,
    'use_ldap' => true,
    'reg_fields' => ['name', 'surname', 'mail', 'country',
                     'institution', 'department', 'phone', 'mobile'],
    'saml2'    => array(
      'SP'       => "https://saml2_service_provider",
      'callback' => "https://rap_IdP_callback"),
    'archive'  => array (
      'dbms'     => "mysql",
      'db'       => "SKA",
      'host'     => "localhost",
      'user'     => "username",
      'secret'   => "password"),
    'ldap'     => array (
      'server'   => "ldap://localhost/",
      'manager'  => "cn=manager,dc=rap,dc=inaf,dc=it",
      'secret'   => "password",
      'dn'       => "dc=rap,dc=inaf,dc=it",
      'version'  => 3,
      'tls'      => true));
```

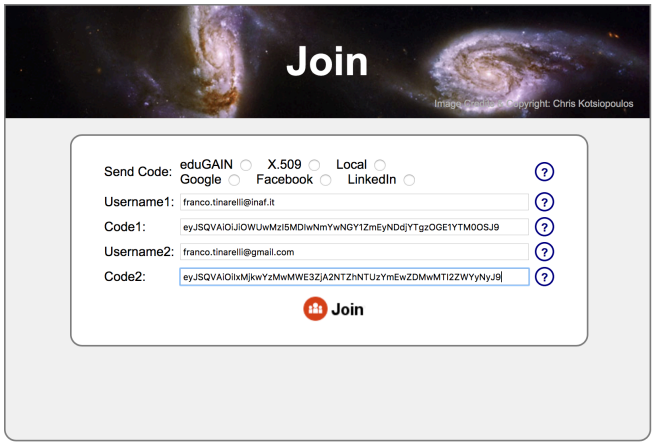
Clients.conf



{"**type**":"**eduGAIN**",”
username":"franco.tinarelli@inaf.it",
"email":"f.tinarelli@ira.inaf.it",
”nome":"Franco","cognome":"Tinarelli",
"org":"INAF","orgu":"IRA","nazione":"IT",
"cel":"NA","tel":"NA",
"**join**":[{"type":"**Google**",
"username":"franco.tinarelli@gmail.com",
"mail":"franco.tinarelli@gmail.com"}]}

json restituito





RAP - Caratteristiche:

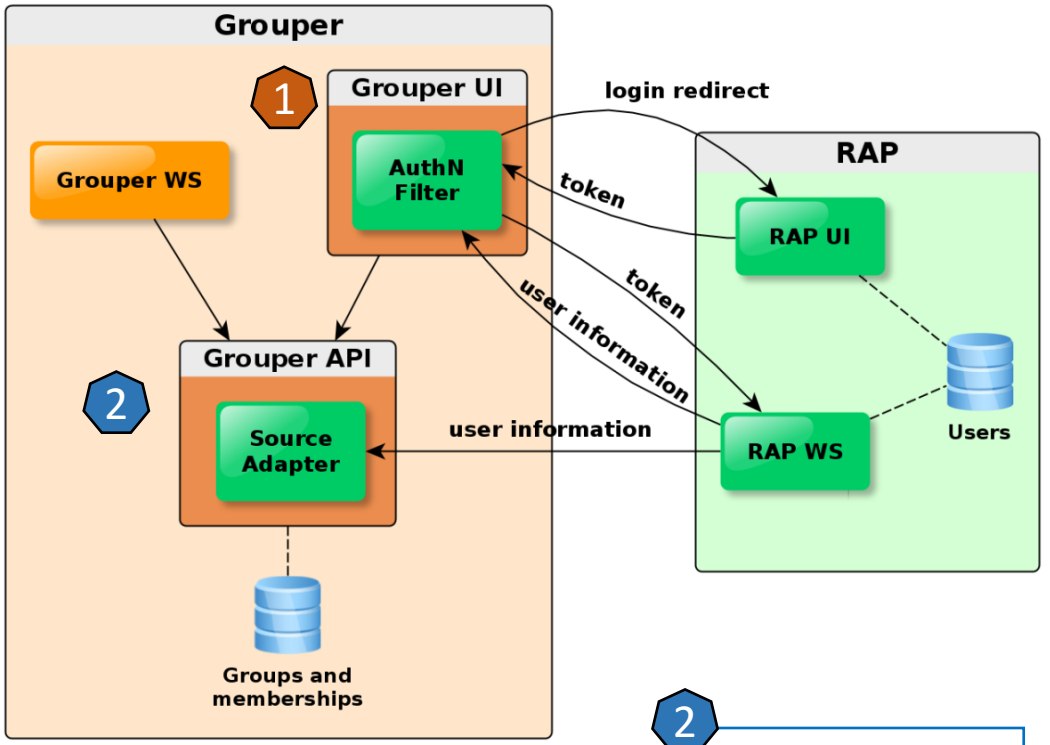
- RAP è un'applicazione web sviluppata in PHP che permette l'autenticazione con diversi sistemi, SAML2 (eduGain), OAUTH2 (Google, Facebook, LinkedIn), X509 (certificati personali IGTF, TERENA-TACAR);
- Può registrare gli utenti in DBMS o LDAP o può passare le informazioni di autenticazione senza registrare gli utenti. I DB possono essere locali, presso il servizio richiedente, presso terzi;
- Se gli utenti vengono registrati diventa possibile unire le diverse identità, modificare i propri dati, o abilitare gli utenti a login SSH via LDAP e/o Kerberos;
- L'unione delle identità può avvenire utilizzando i token inviati via email dopo il primo login registrato;
- È indipendente dal servizio che richiede l'autenticazione, il servizio deve comunque essere conoscito e descritto in un file di configurazione;
- Nel file di configurazione il servizio può spegnere e accendere le opzioni di login e i DB da utilizzare, deve specificare l'indirizzo di ritorno dei dati di autenticazione;
- I dati vengono inviati o direttamente al servizio, o inviando un token col quale è possibile richiederli.

Provatelo all'indirizzo **https://rap.inaf.it/Services/RAP**

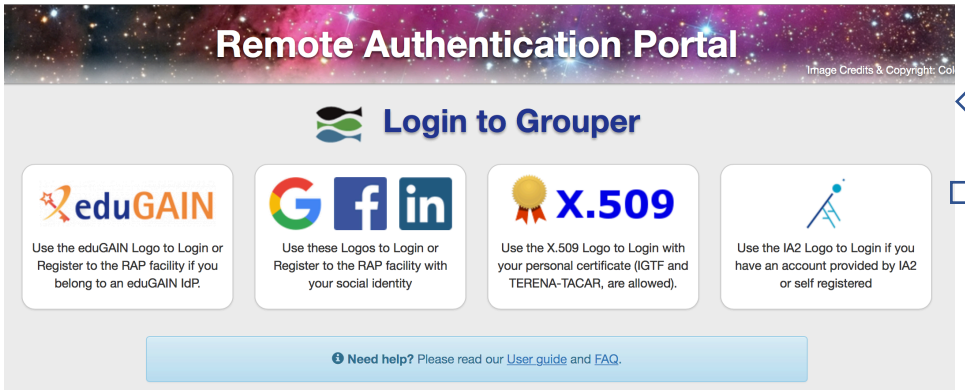
RAP + Connettori = RAP + Grouper

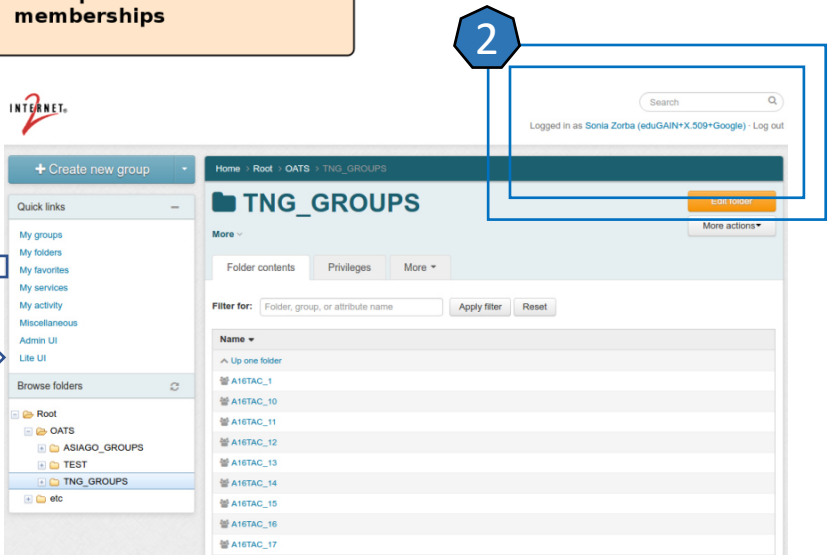
Grouper non è in grado di autenticare gli utenti utilizzando RAP ed è stato necessario modificare l'**Authentication Filter** 1

Grouper non è in grado di capire il concetto di "identità unite" ed è stato necessario modificare il **Source Adapter** per recuperare da RAP le informazioni utente. 2



https://sso.ia2.inaf.it/ **(Provatelo!)**

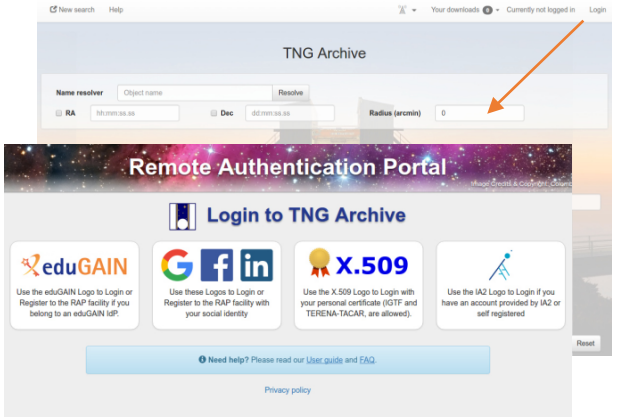


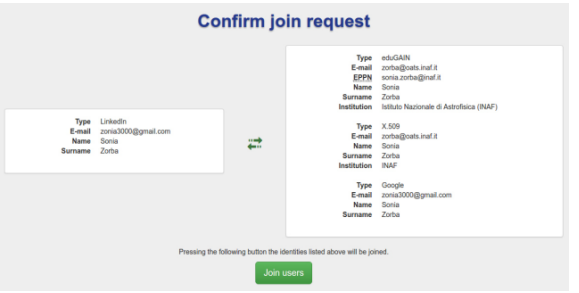


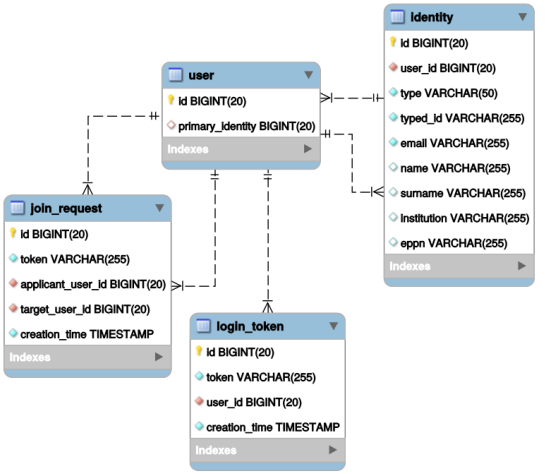
RAP + Grouper :

- Già operativo come sistema di Autenticazione e Autorizzazione degli archivi delle osservazioni astronomiche e radioastronomiche;
- Sono state modificate due classi java di Grouper per permettere l'autenticazione con RAP e il riconoscimento di identità unite;
- L'unione di identità avviene inviando una email contenente un link di conferma alla email dell'identità da unire;
- I dati utente vengono recuperati dal servizio utilizzando il token ricevuto da RAP;

- I codici sorgente sono distribuiti con licenza GPLv3:
  - RAP: https://www.ict.inaf.it/gitlab/zorba/rap-ia2
  - Modifiche per Grouper: https://www.ict.inaf.it/gitlab/zorba/rap-grouper







GRAZIE PER L'ATTENZIONE

Domande?