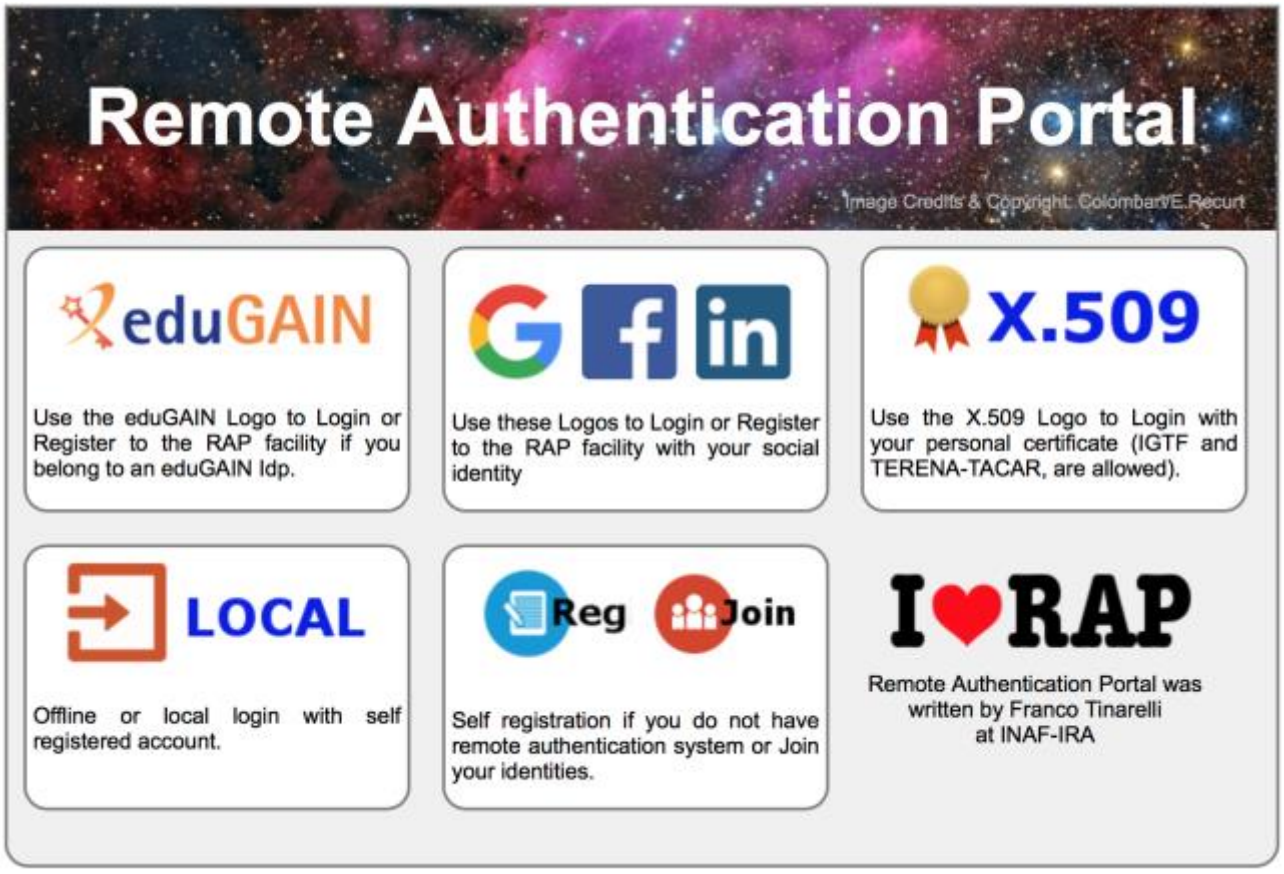
Accesso ai dati astronomici e radioastronomici, l'approccio di INAF al problema dell'Autenticazione e Autorizzazione.

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. Essa permette inoltre l'account linking ed ha un connettore 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. Esso inoltre ha il vantaggio di fornire un'interfaccia web che consente di delegare agli utenti alcune delle operazioni di amministrazione dei gruppi. Grouper non è nativamente in grado di gestire l'account linking, e la relativa autorizzazione per questo è stato necessario personalizzarne alcune componenti, in modo da renderlo compatibile con il modello dati utilizzato da RAP per rappresentare gli utenti. L'implementazione di un meccanismo di autenticazione multi protocollo (SAML2.0, OAuth2, X.509), la registrazione automatica su DBMS, LDAP e Kerberos, l'account linking delle identità e la gestione di gruppi di utenti permette oggi l'accesso ai dati prodotti dagli strumenti osservativi di INAF e permetterà in futuro l'accesso alla impressionante mole di dati prodotta dal radiotelescopio SKA.

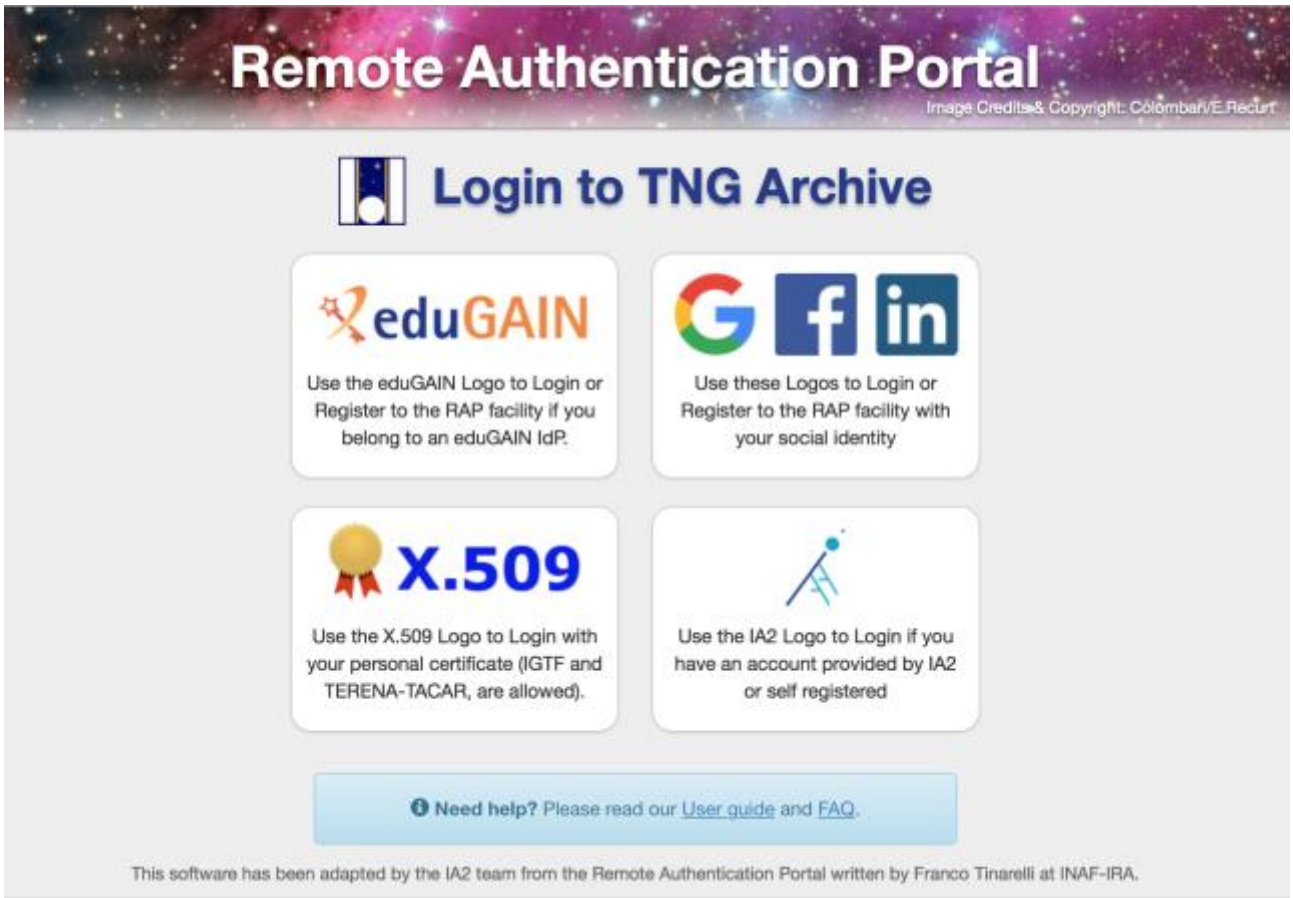


RAP (Remote Authentication Portal) è un'applicazione web scritta in PHP, è completamente indipendente dalle applicazioni che lo usano come autenticatore.

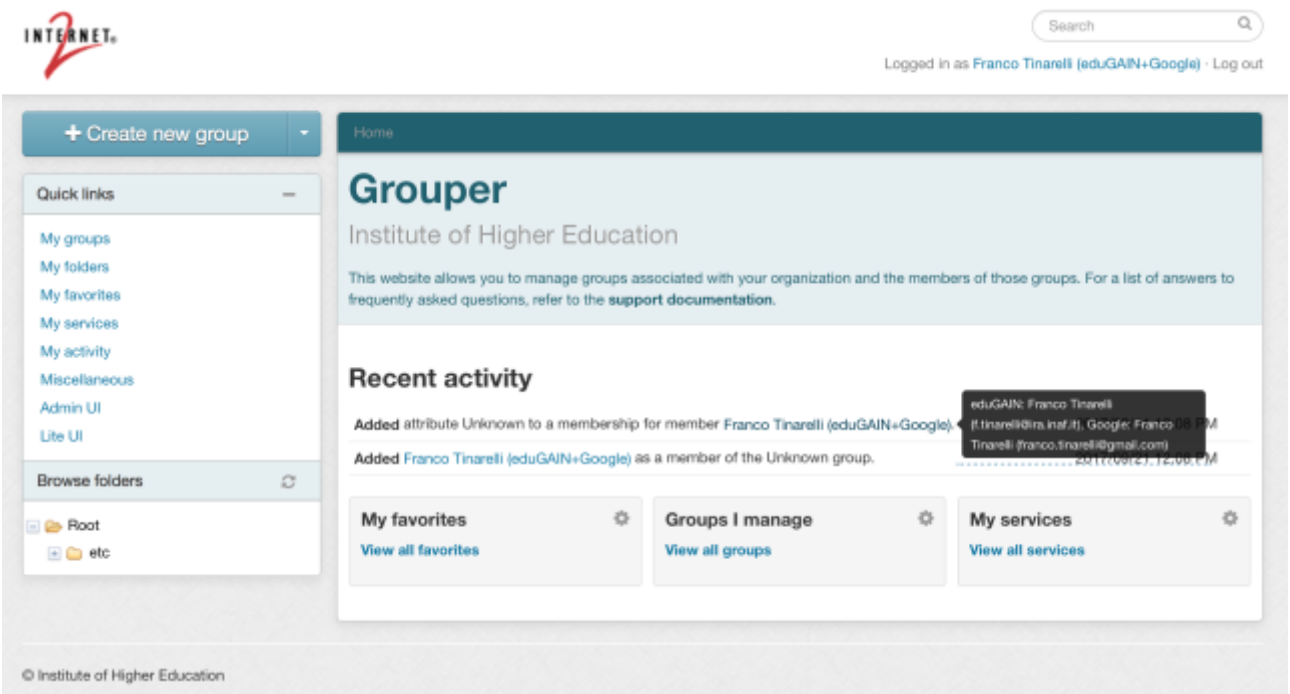
L’applicazione chiamante viene registrata in un file che contiene l’indirizzo di call-back per ritornare i dati dell’utente che si e’ autenticato.
Le principali funzionalità del programma sono:

1. autenticazione con diversi metodi,
2. account-linking,
3. registrazione in MySQL o LDAP,
4. editing dei profili registati.

Ciascuna delle funzionalità possono essere attivate/disattivate a piacimento e nel secondo caso vengono nascoste nell’interfaccia utente. Il meccanismo di autenticazione viene reso più sicuro tramite l’associazione della richiesta di autenticazione ad un token inviato all’applicazione chiamante che lo userà come chiave per richiedere gli attributi di autenticazione, con conseguente eliminazione dei dati transienti e token immediatamente dopo l’invio e salvati nel sistema di audit trail.
La registrazione degli utenti può essere effettuata direttamente da RAP su proprie tabelle associate all’applicazione chiamante o remotamente su DB della stessa applicazione. Analogamente all’indirizzo di call-back anche questi dati vengono associati all’applicazione chiamante in un file di configurazione dei client. RAP può utilizzare indifferentemente un db relazionale o LDAP per la registrazione degli utenti sia in locale che in remoto per la funzionalità di account-linking. L’utilizzo di LDAP permette, attraverso una procedura di gestione, di accreditare gli utenti al login via SSH su workstation che lo utilizzino come sistema di autenticazione. Successivamente la stessa funzionalità può esser estesa all’utilizzo di Kerberos per quelle applicazioni che ne richiedessero l’utilizzo.
RAP è Open Software e può essere adattato e inserito in una propria applicazione, come realizzato dal team di IA2.



La suite è completata dal connettore tra RAP e Grouper, sviluppato dal team IA2 che permette l'autenticazione su grouper tramite l'utilizzo di un sistema multi protocollo che non era nativamente supportato da Grouper. Grouper con la modifica apportata alla sua nativa basic authentication, importa da RAP le diverse identità possedute dall'utente che si è autenticato come un'unica, per gestire i gruppi di cui è amministratore. RAP espone queste informazioni attraverso un servizio REST protetto da password.
Due moduli di Grouper sono stati personalizzati per poter dialogare con questo web service: il Source Adapter e l'Authentication Filter. La creazione di questi componenti custom avviene estendendo delle classi Java, modificando i file XML della configurazione di Grouper e infine ricompilando Grouper.
Nel gergo di Grouper un Source Adapter è un componente che può essere interrogato per ricavare informazioni riguardo un insieme di utenti. Ogni installazione di Grouper può avere uno o più Source Adapter. I Source Adapter messi a disposizione da Grouper permettono di interrogare LDAP o database relazionali. Il Source Adapter scritto da IA2 interroga invece il servizio REST di RAP, che restituisce le informazioni in formato JSON. In questo modo un insieme di identità sulle quali è stata effettuata una procedura di account linking viene interpretato da Grouper come un'entità atomica. Nella Grouper UI, a fianco del nome di ogni utente vengono elencate le sue diverse identità.
L'Authentication Filter è un servlet filter che va configurato nel deployment descriptor della Grouper UI. Verifica la presenza di un utente associato al cookie di sessione, in caso contrario effettua un redirect su RAP e si autentica allo stesso modo degli altri client.



Franco Tinarelli[1], Sonia Zorba[2], Cristina Knapic[2]
1 – INAF Istituto di Radioastronomia; 2 – INAF Osservatorio Astronomico di Trieste;