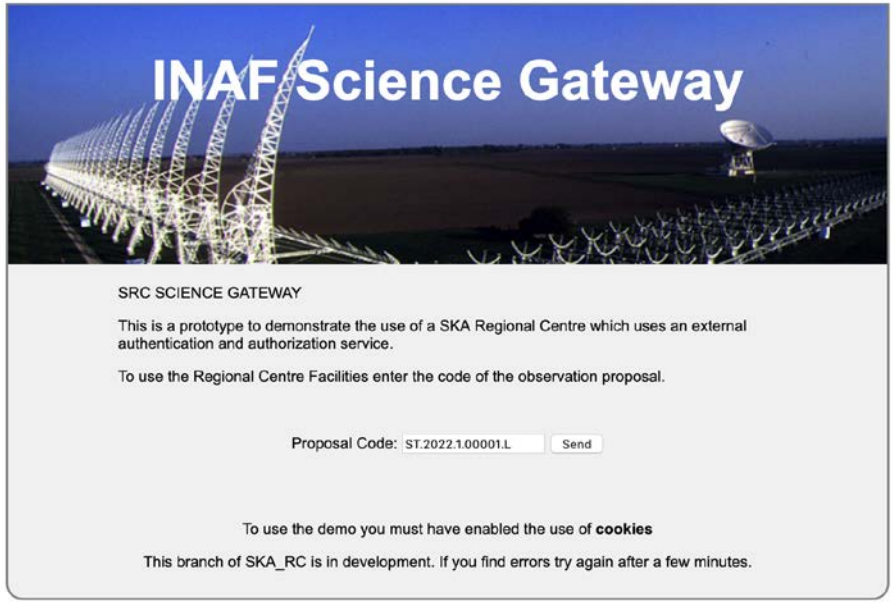
Science Gateway Prototype

F. Tinarelli, C.Knapic, S. Bertocco, S. Zorba, G. Taffoni

Prototype use case for SKA RC

INAF
ISTITUTO NAZIONALE DI ASTROFISICA
NATIONAL INSTITUTE FOR ASTROPHYSICS

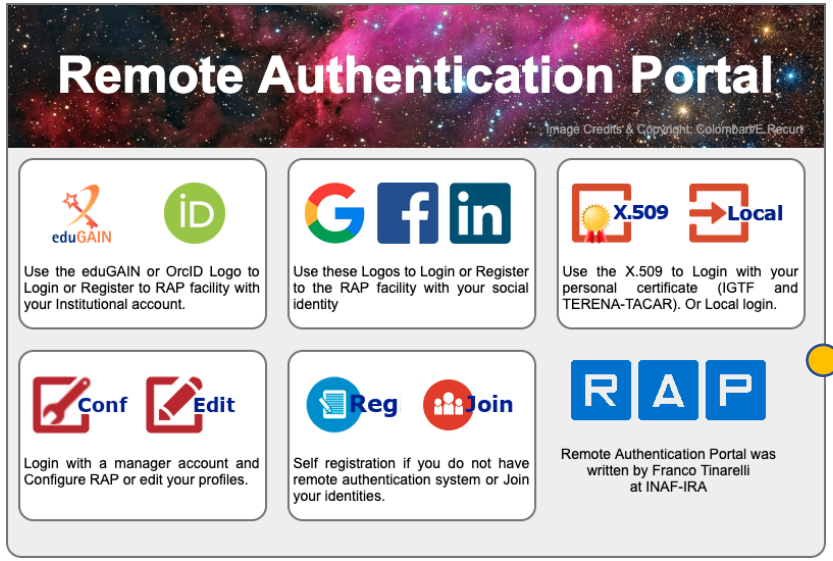
SKA SQUARE KILOMETRE ARRAY Partner (design)



Science Gateway Catalog
IN: proposalID
OUT: IVO-ID, Data_Center, files, ivo://authority.org/path?groupID

IN: Authentication

OUT: User Unique ID



Data Center (Archive+Computation)
Token exchange
Data access and computation

Containers Repository

IA2/GMS

Grouper/GMS
IN: groupID, user_unique_ID
OUT: authorization

Grouper™

IVOA

eneas

Actors: The Science Gateway

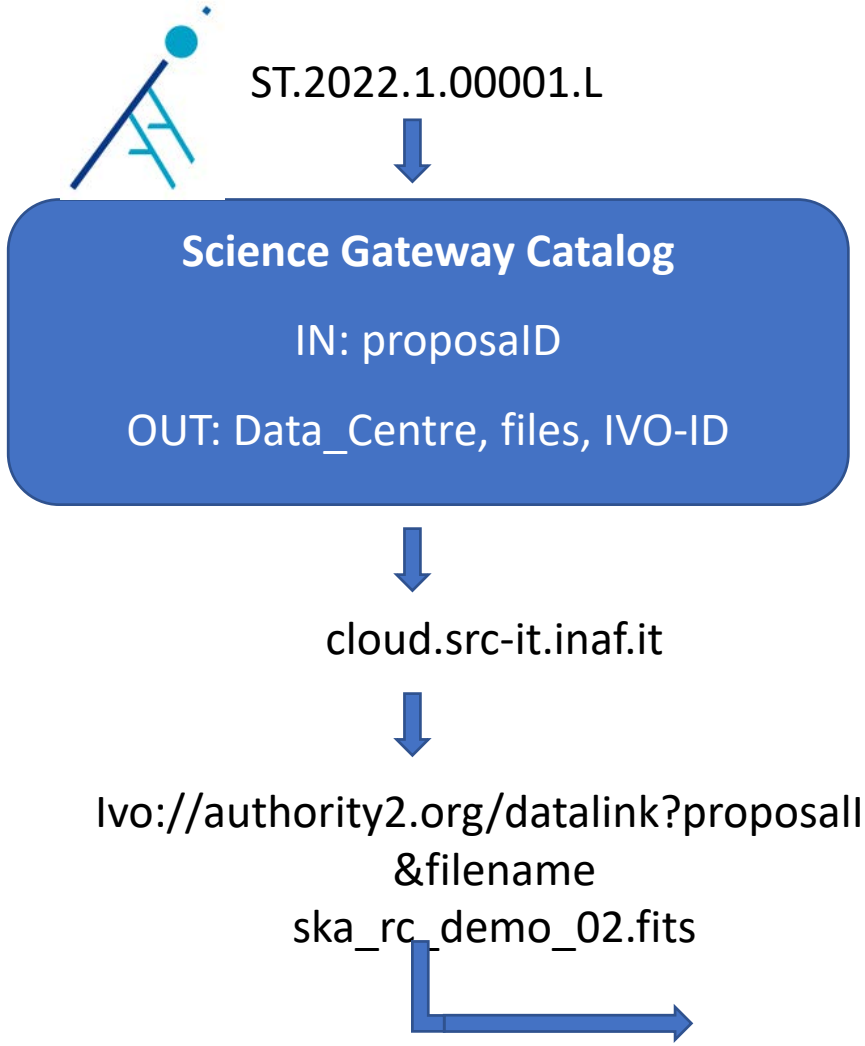
- The Science Gateway is the entry point of the data retrieval
- It is able to query the archive of observational data using standard VO queries
- It is usually dedicated to observational projects of one Organization
- If the syntax of the proposal_ID become a standard, it could serve observational projects of more Organizations

Instrument
Year
Cycle
number++
Type

ST.2022.1.00001.L

ALMA syntax

Actors: The Science Gateway Catalog



The catalog contains information encoded using IVOA notation.

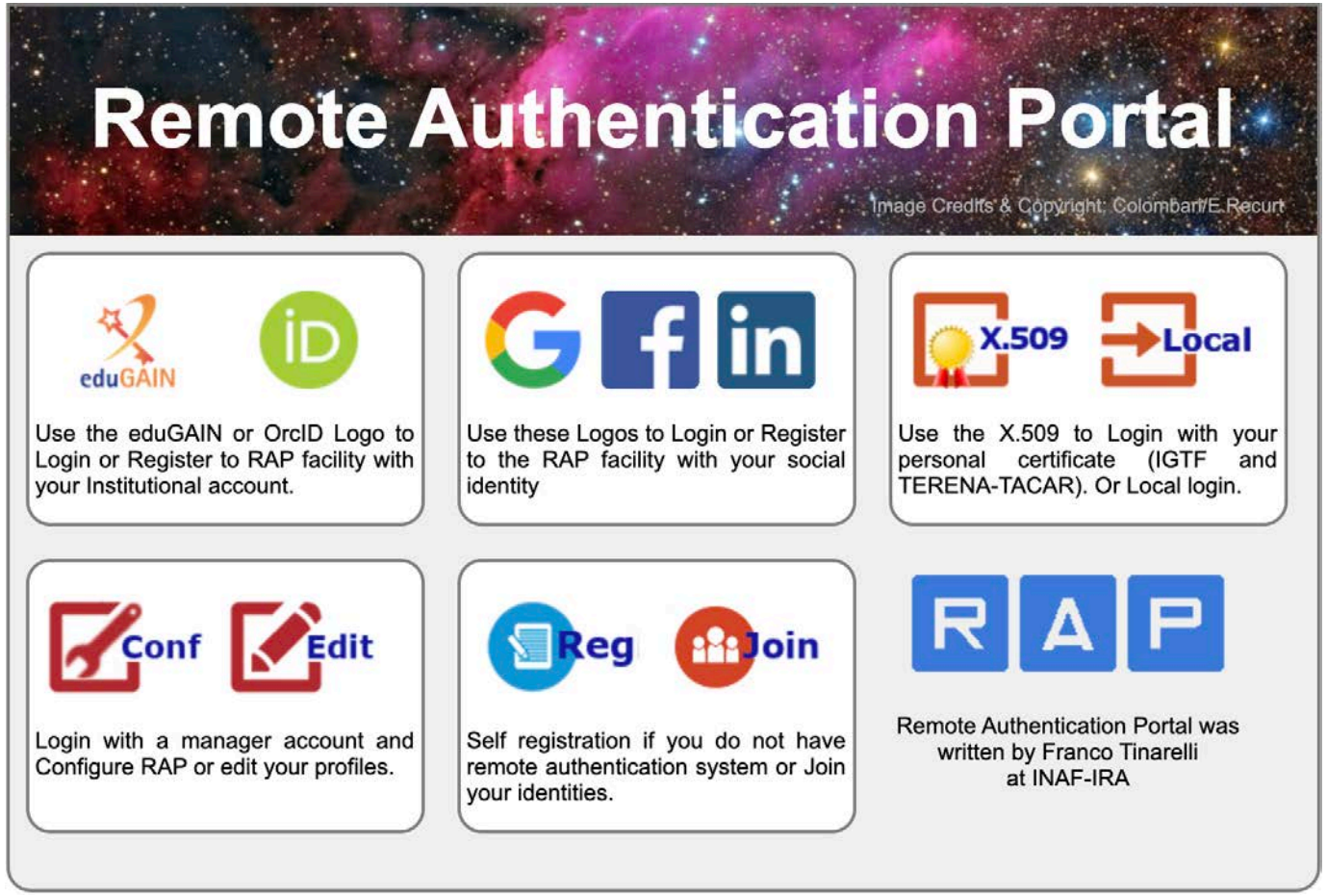
Group identifiers follow the GMS (current draft) specification, that embeds:

- authority: managing the group management service
- service identification: to call for authZ purposes (The authN is not currently defined but it is being studied)
- The group ID of the proposal dataset belongs to

ivo://authority.org/path?groupID

(ivo://auth.ska.org/grouper?ST_2022_1_00001_L)

Actors: The Remote Authentication Portal (RAP)

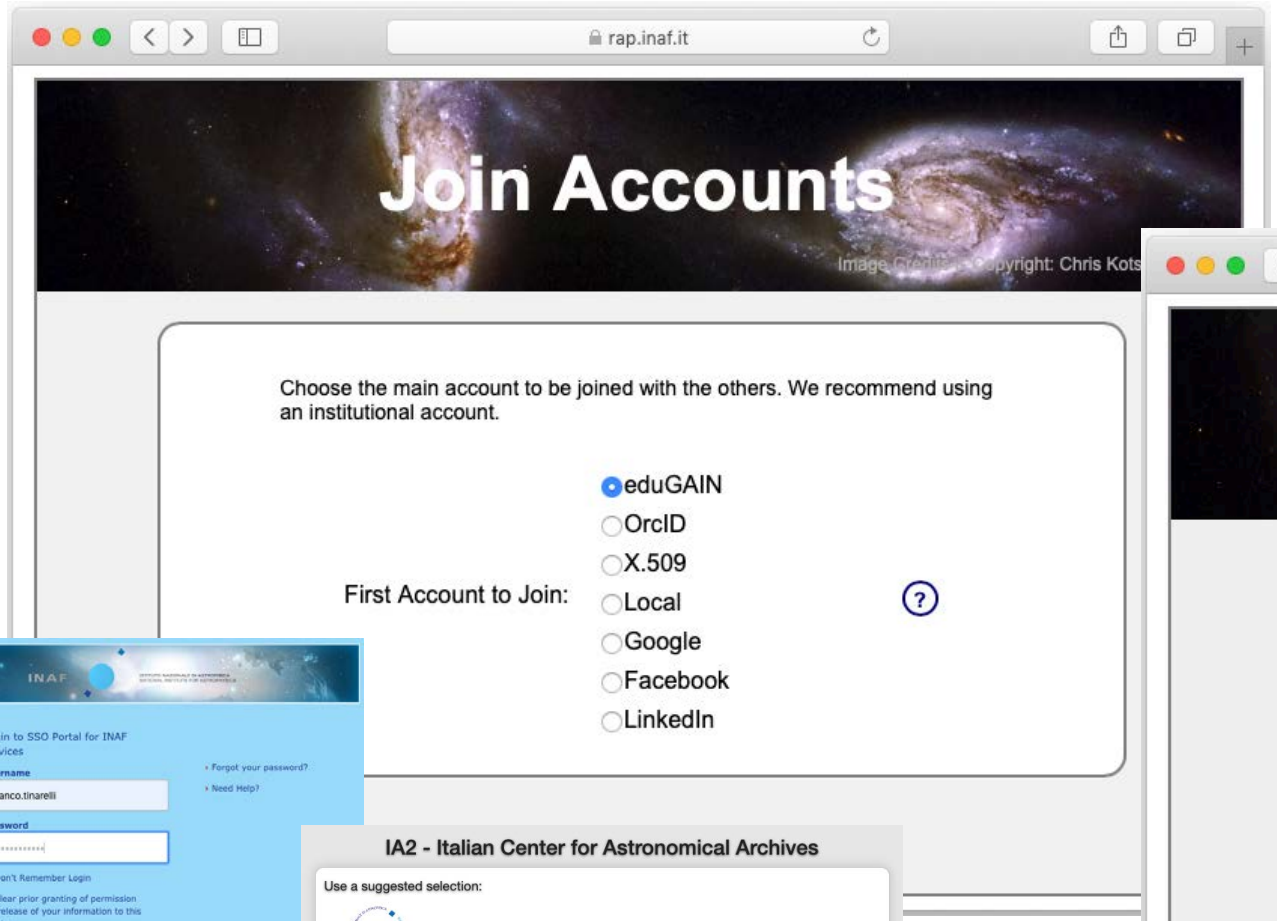


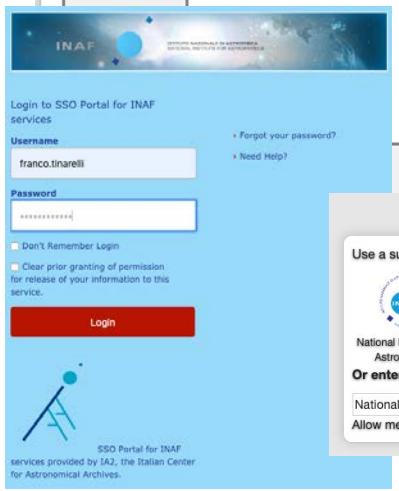
(Use the link https://rap.inaf.it/Services/DEMO to test a fully functioning demonstration.)

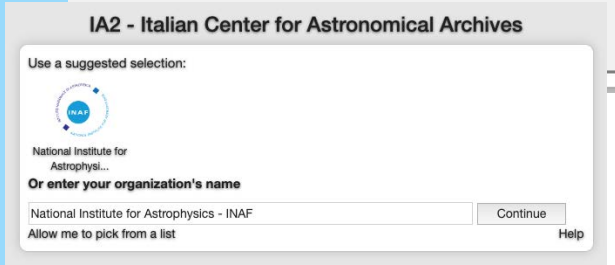
- RAP is an Authentication system built by INAF capable to handle multiple accounts for web application usage
- Born as a SKA Pre-construction phase component - a joint venture between Radio Astronomical Institute (IRA) and Italian Astronomical Archives (IA2)
- The first RAP prototype has been presented at the "SKA TM prototype strategy" meeting in Trieste in march 2015
- RAP is used in the production portal of IA2 in conjunction with Grouper since 2017
- The current RAP version is able to join the different user accounts into a single entity (Account Linking)
- RAP use OAuth2 and OpenID Connect to communicate with the Science Portal or other clients

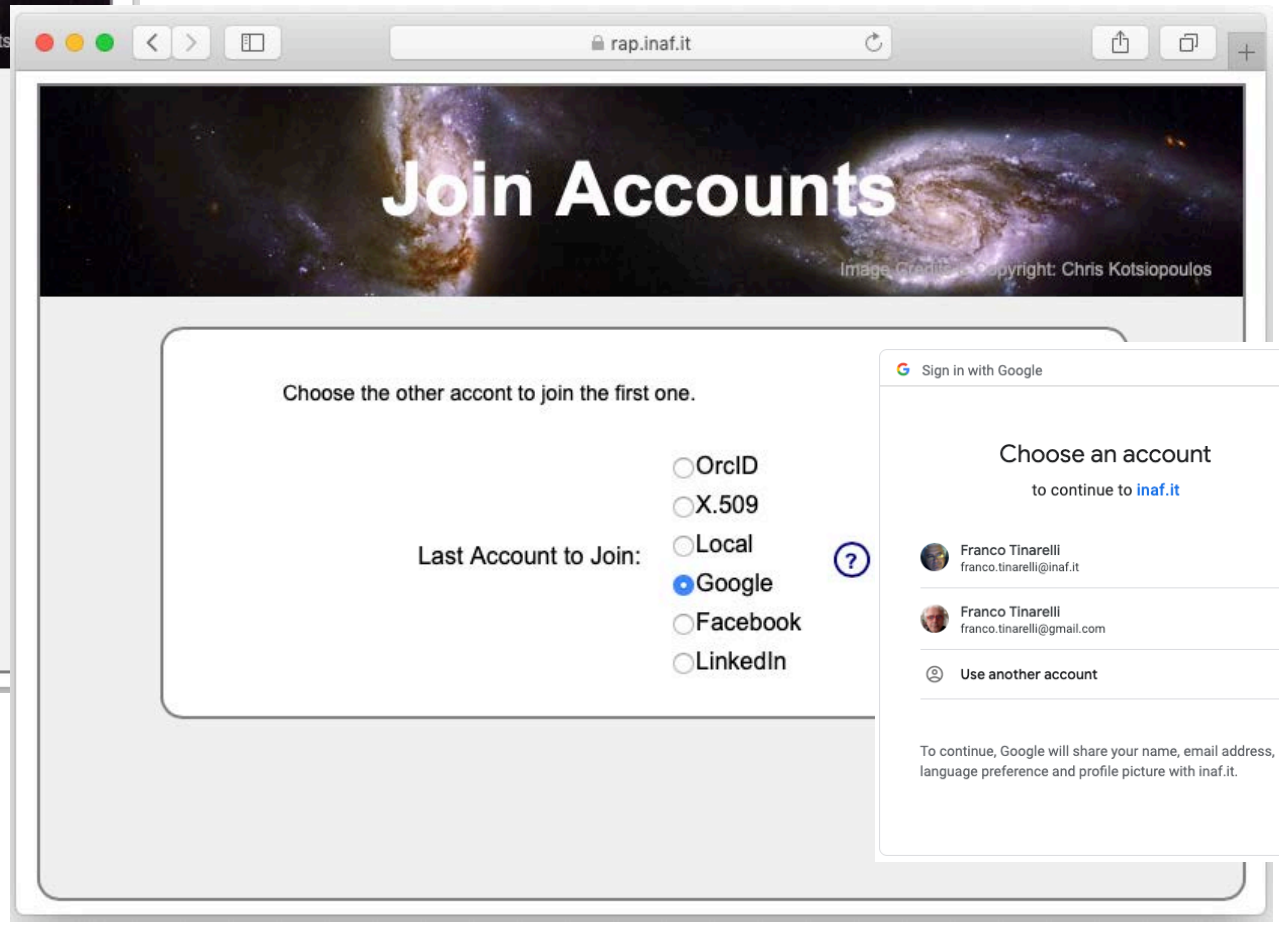
Actors: RAP and Account Linking

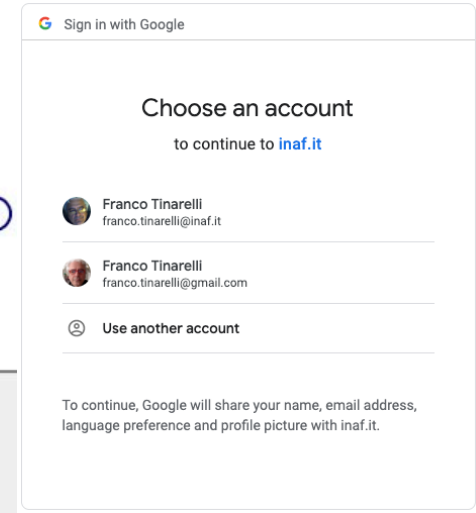
- The join operation requires the user to always authenticate himself **for security reasons** to his different identities.
- It is strongly suggested to choose an istitutional account as the reference one to join against to.



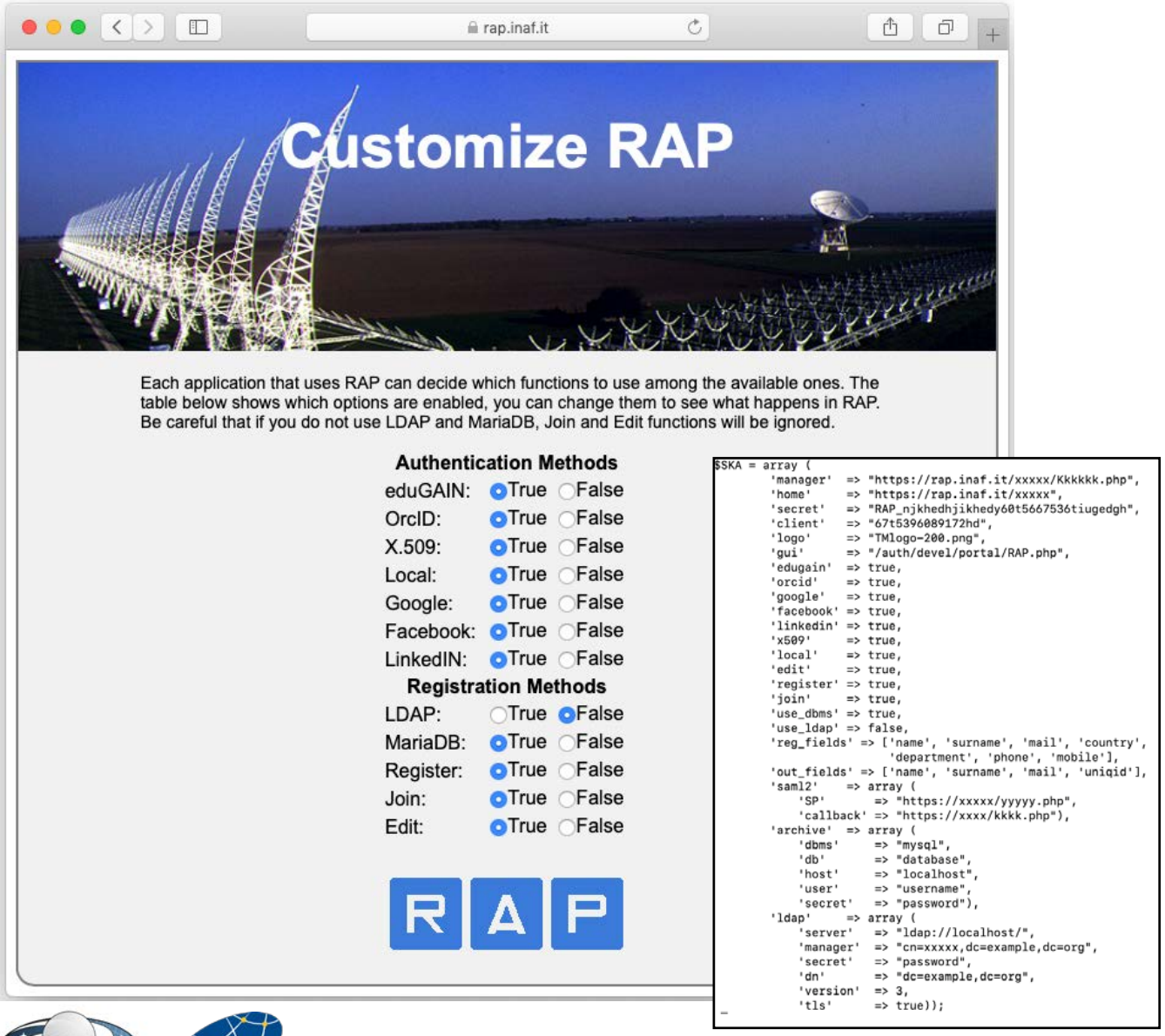








Actors: RAP and the DEMO Customization




```
$SKA = array (
        'manager'  => "https://rap.inaf.it/xxxxx/Kkkkkk.php",
        'home'     => "https://rap.inaf.it/xxxxx",
        'secret'   => "RAP_njkhedhjikhedy60t5667536tiugedgh",
        'client'   => "67t5396089172hd",
        'logo'     => "TMlogo-200.png",
        'gui'      => "/auth/devel/portal/RAP.php",
        'edugain'  => true,
        'orcid'    => true,
        'google'   => true,
        'facebook' => true,
        'linkedin' => true,
        'x509'     => true,
        'local'    => true,
        'edit'     => true,
        'register' => true,
        'join'     => true,
        'use_dbms' => true,
        'use_ldap' => false,
        'reg_fields' => ['name', 'surname', 'mail', 'country',
                         'department', 'phone', 'mobile'],
        'out_fields' => ['name', 'surname', 'mail', 'uniqid'],
        'saml2'    => array (
            'SP'       => "https://xxxxx/yyyyy.php",
            'callback' => "https://xxxx/kkkk.php"),
        'archive'  => array (
            'dbms'     => "mysql",
            'db'       => "database",
            'host'     => "localhost",
            'user'     => "username",
            'secret'   => "password"),
        'ldap'     => array (
            'server'   => "ldap://localhost/",
            'manager'  => "cn=xxxxx,dc=example,dc=org",
            'secret'   => "password",
            'dn'       => "dc=example,dc=org",
            'version'  => 3,
            'tls'      => true));
```

RAP is a Proxy between applications and identity providers or local registration

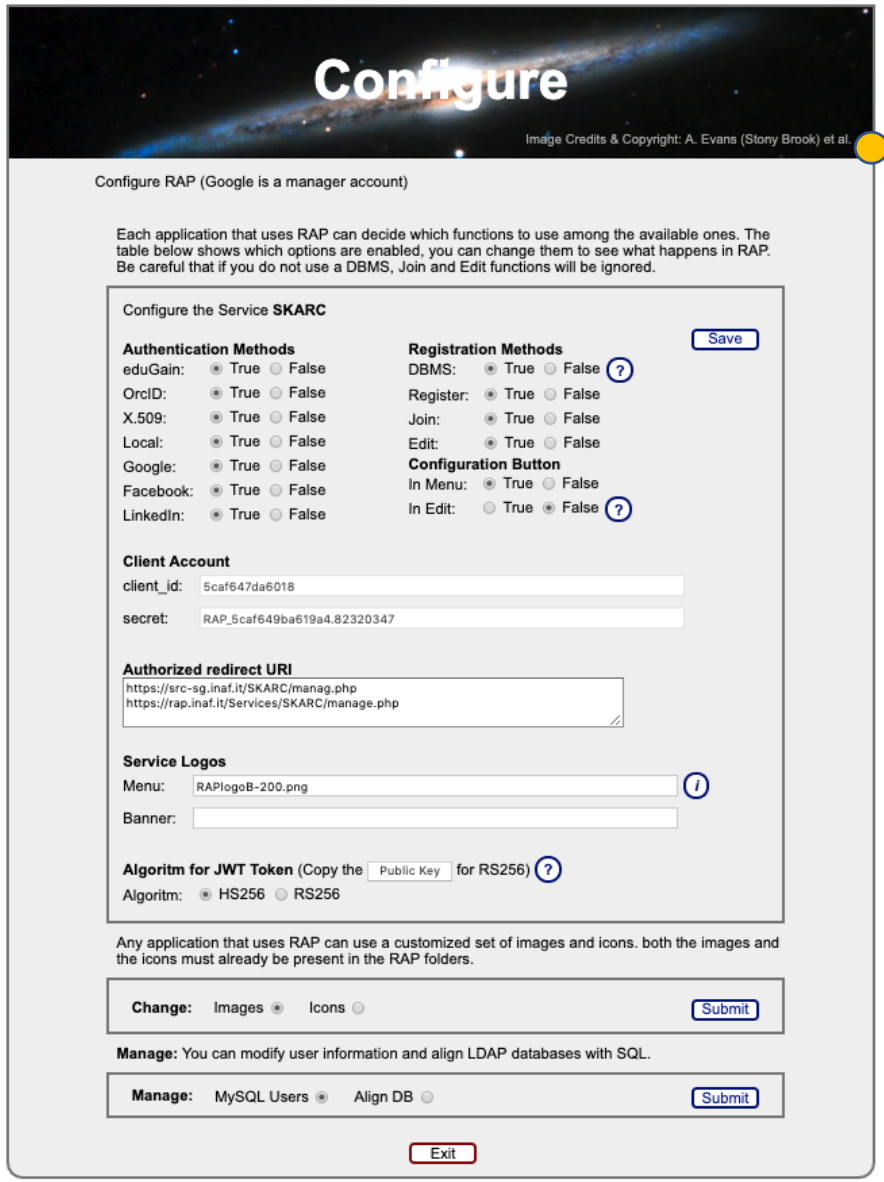
It can be customized from applications (through configuration file):

- Supported providers can be chosen
- Support for local user registration, and X.509 authentication
- It can be configured as pass-through authenticator without user registration
- LDAP and/or SQL Servers for user registration at first login (required for account linking) are supported
- LDAP and/or SQL Server DBs can be called locally by RAP or remotely
- RAP is Open Source. It can be installed as a local service or used as a network service

Actors: RAP the Config Command

RAP General Manager:

- Select and Configure all registered Services;
- Manage LDAP users, SQL users and Align DB;
- Create new Service and add a Service Manager;



RAP Service Manager:

- Configure the layout of Service;
- Read Client ID and Secret;
- Add or Remove Authorized Redirect URI;
- Select The Service Logos;
- Select the Algoritm of JWT token and download the Public Key for RS256;
- Change the Top Page Images and Menu Icons;
- Manage SQL users and Align SQL and LDAP informations;

Actors: The Science Gateway GMS

ST_2022_1_00001_L / 10001

↓

5333031393130323 2f7ce4ea1@rap.inaf.it

↓

Grouper/GMS
IN: groupID, user_unique_ID
OUT: authorization

↓

Grouper™

Authorization →

- The Group Management System contains information about the group that owns the requested proposal_ID
- The group is defined by a group name (alphanumeric) and/or a group ID (numeric). Grouper uses only a numeric ID.
- If the Unique_ID of an authenticated user belongs to the group associated to the proposal_ID, then an authorization is issued.
- the authorization contains a group_ID and can contain a list of privileges associated with the unique_ID belonging to the group.

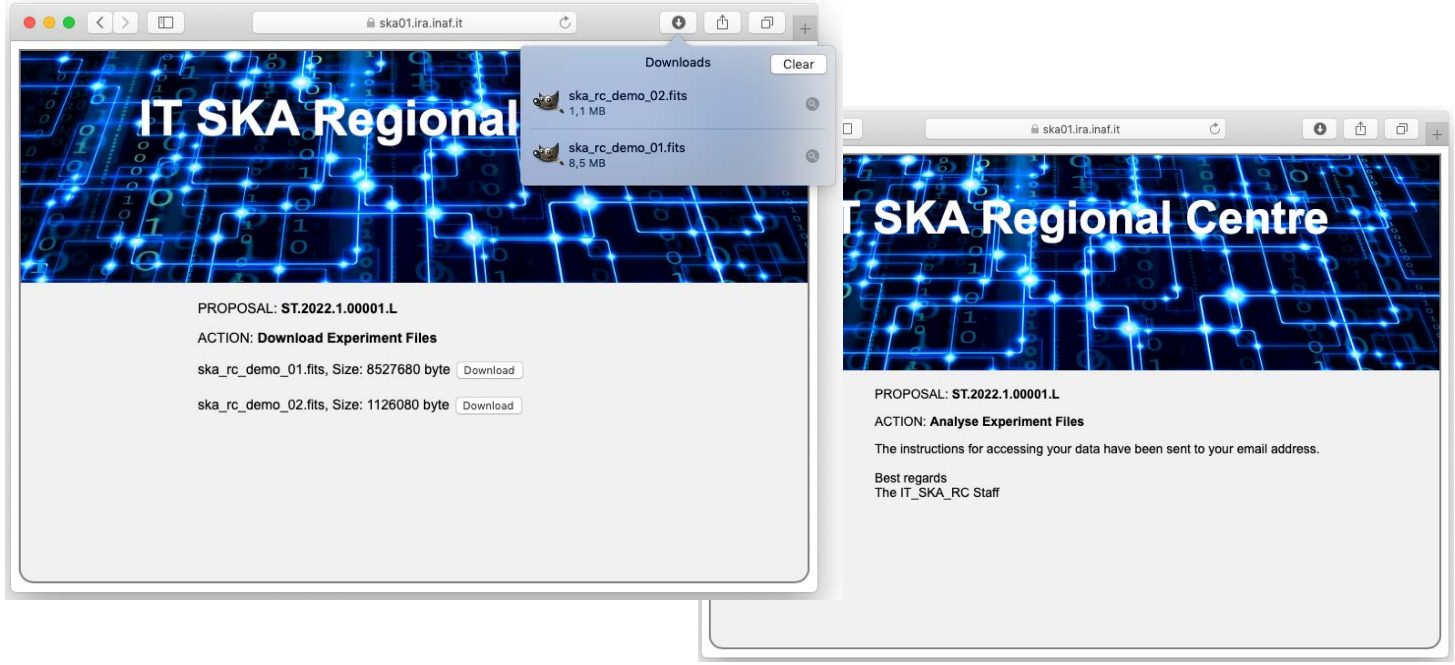
Actors: The Data Centre

Token exchange with Science Gateway

Data Centre (Archive+Computation)
Token exchange
Data access and computation

Access to Data and Computational resources

- The Data Centre exchanges the authorization token with the Science Gateway.
- The token exchange (draft-ietf-oauth-token-exchange-16) is different from the access token used for user authentication. The token is signed with a new client_id and a new secret/keys.
- The Data Centre receives the information about data, groups, and user requests.
- The Data Centre instantiates resources for data transfer or analysis.



The Prototype Step by Step (1)

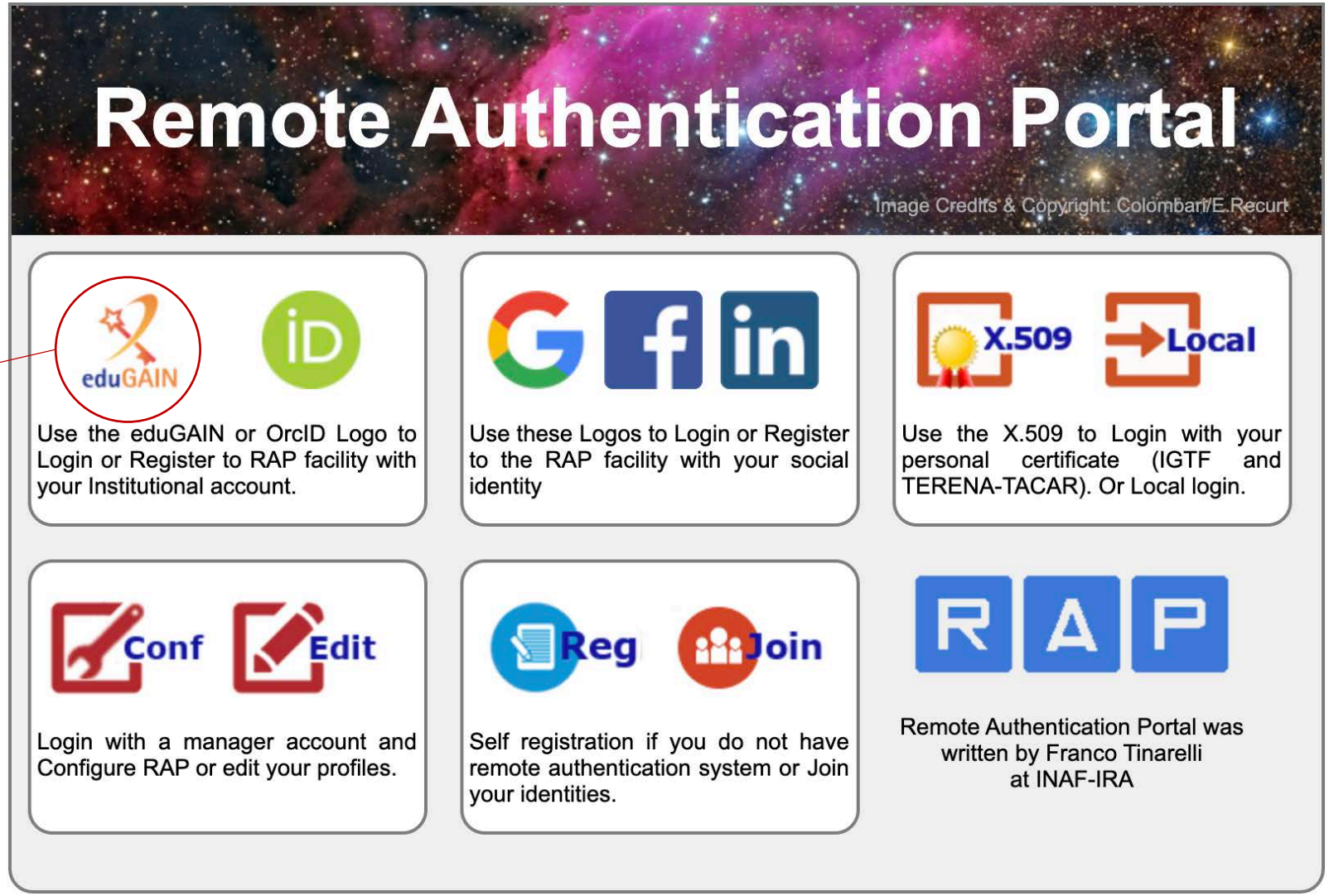
Call Science Gateway

And

Insert the Proposal ID

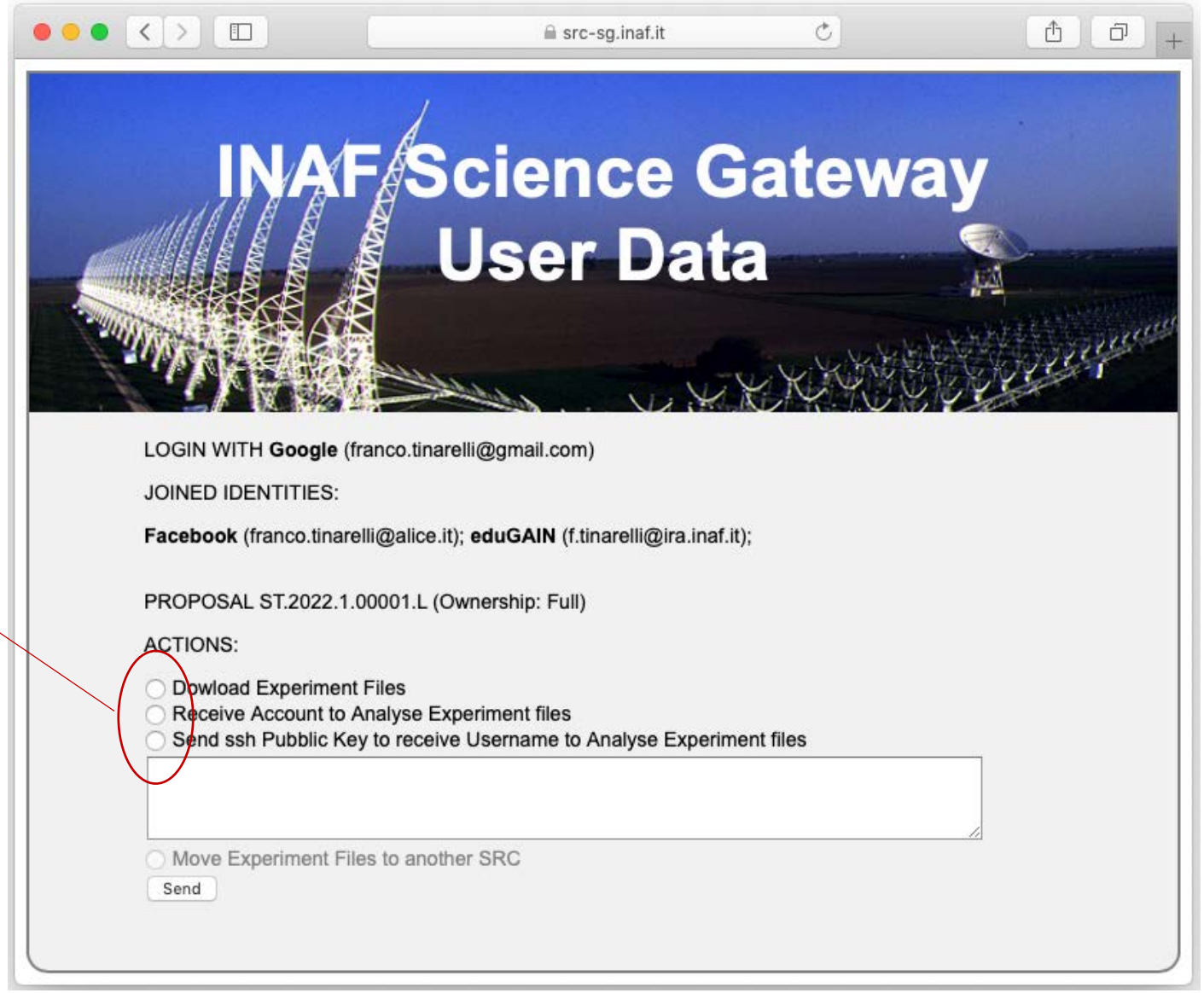
The Prototype Step by Step (2)

Authenticate Yourself



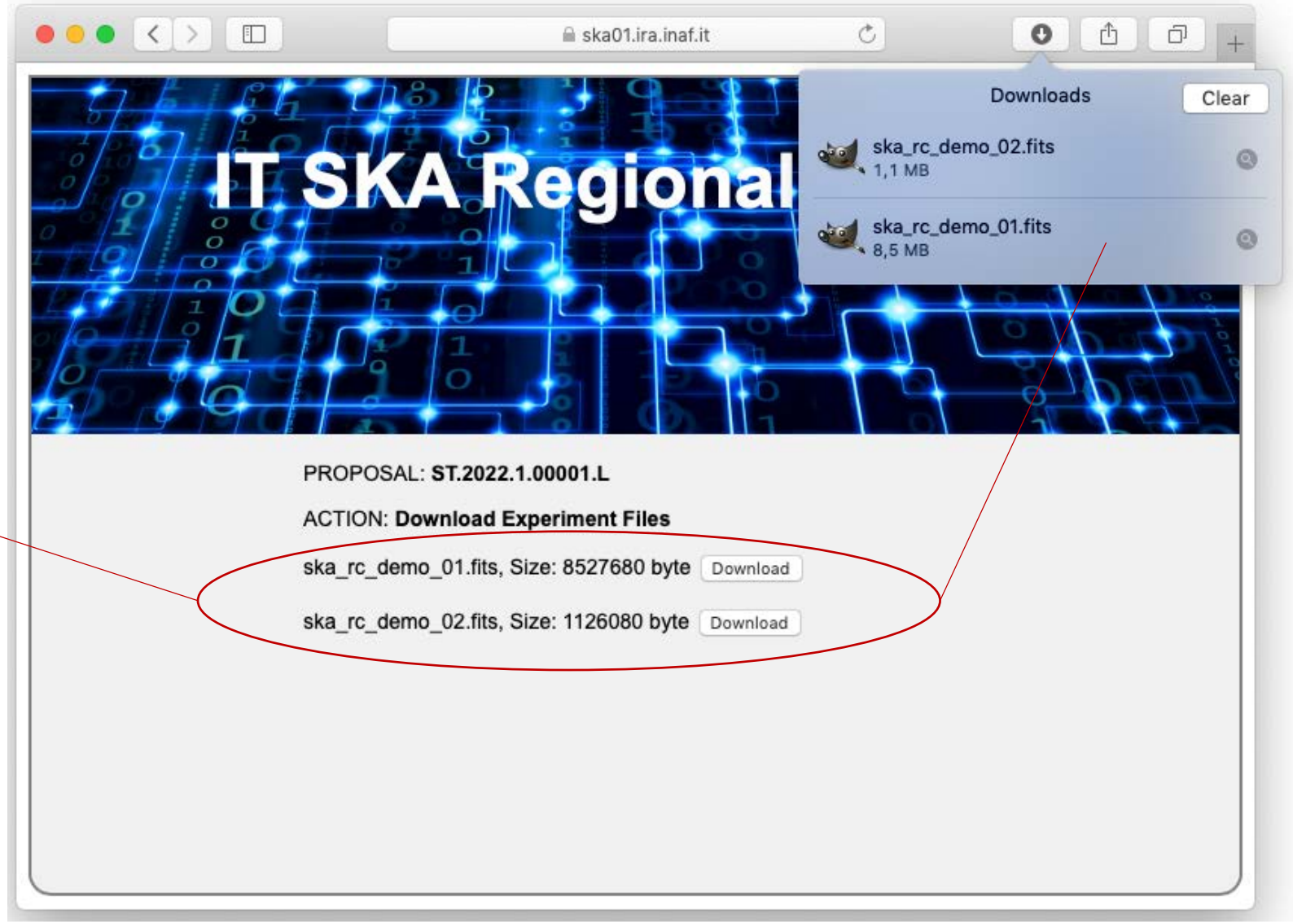
The Prototype Step by Step (3)

Select the actions to manage your data



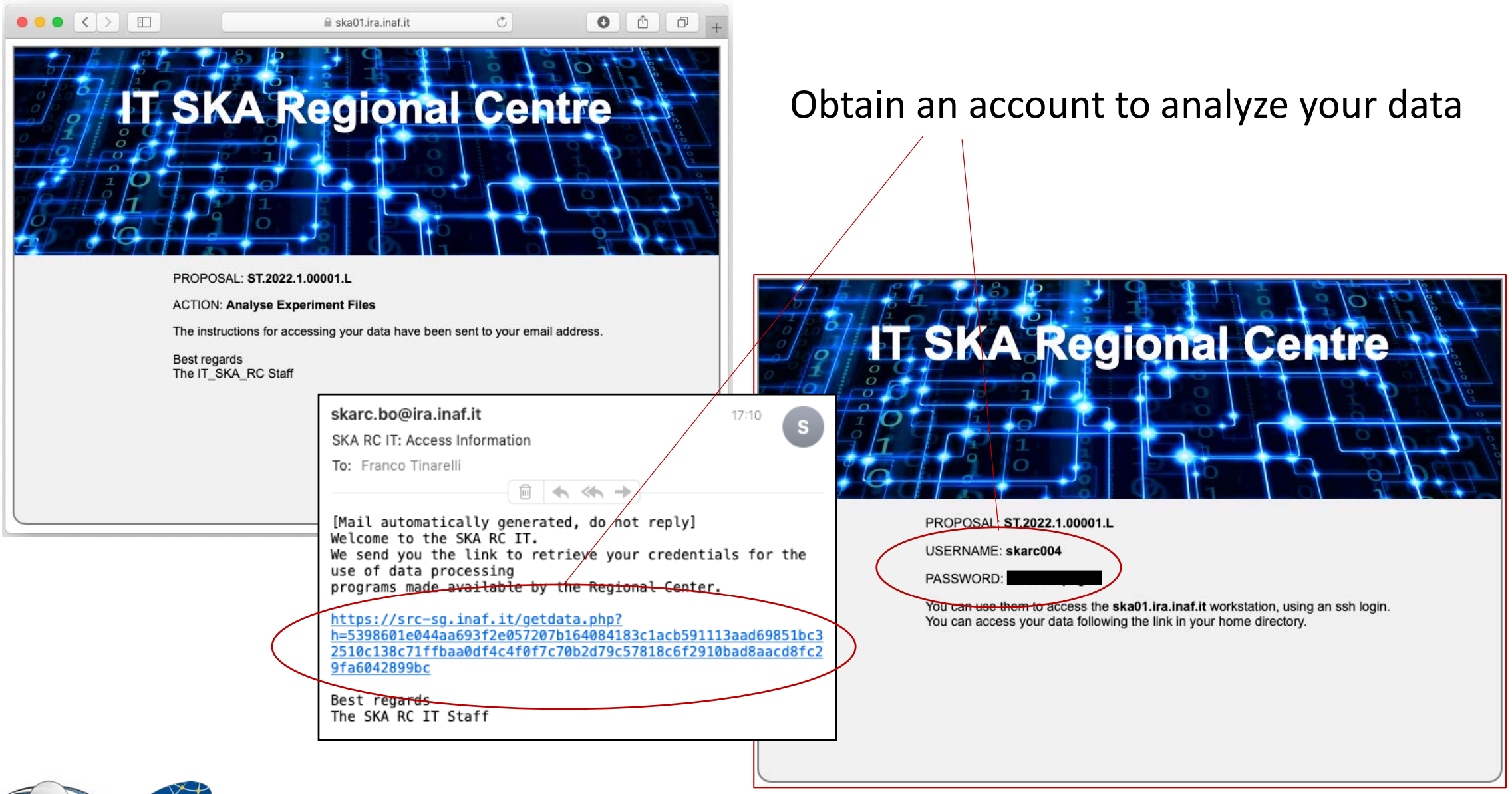
The Prototype Step by Step (4.1)

Dowload experiment files



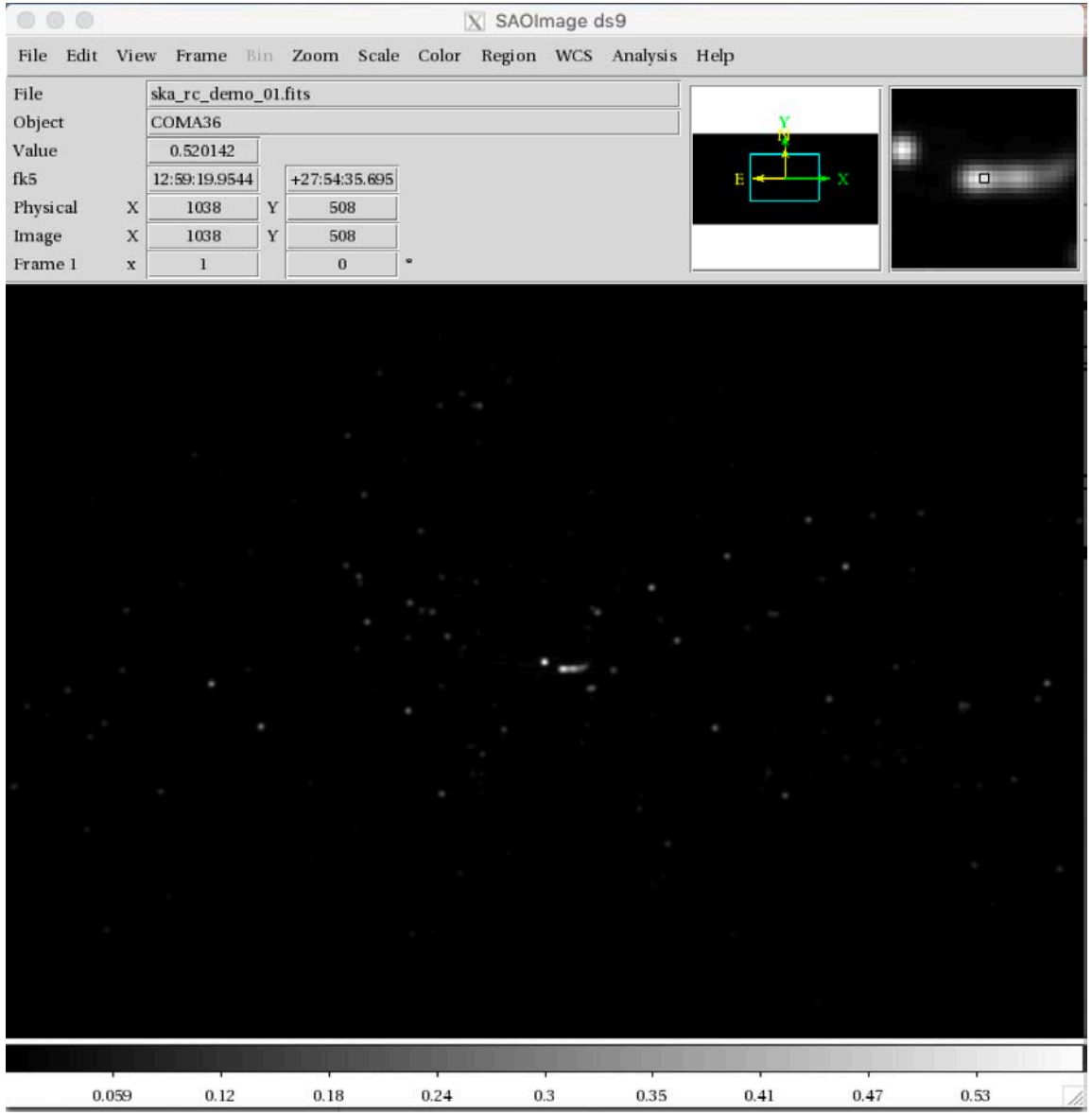
The Prototype Step by Step (4.2)

Obtain an account to analyze your data



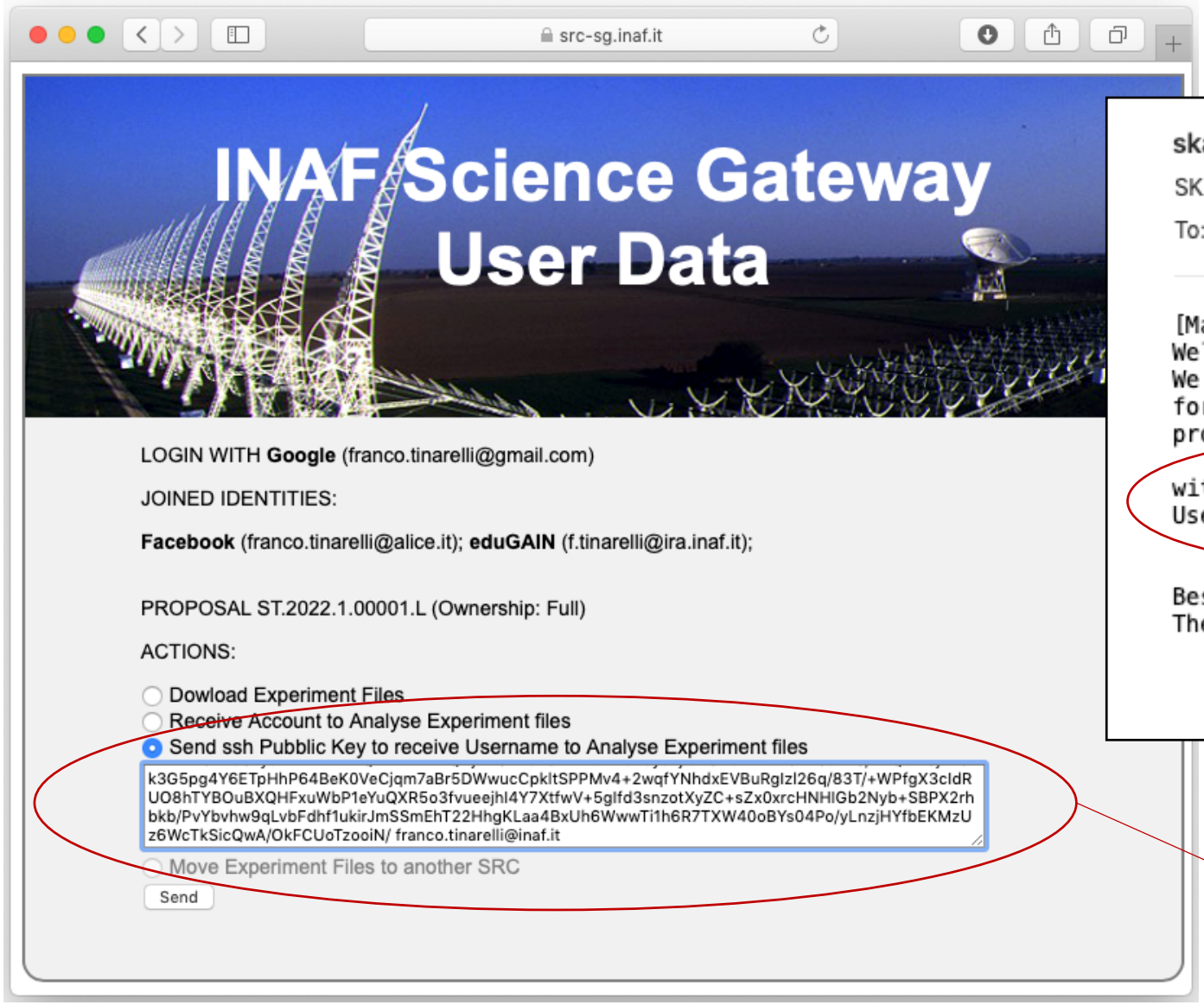
The Prototype Step by Step (4.2.1)

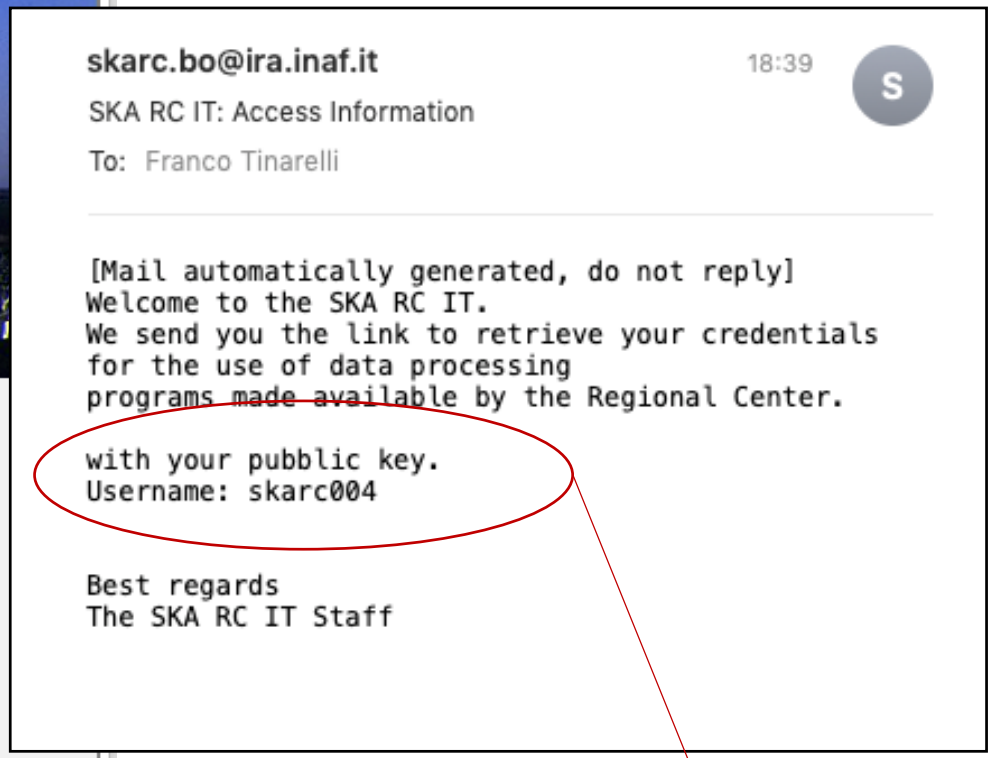
```
bertocco — skarc001@ska01:~/data — ssh -XY skarc001@ska01.ira.inaf.it — 80×24
Last login: Mon May  6 12:35:58 on console
rumba:~ bertocco$ ssh -XY skarc001@ska01.ira.inaf.it
The authenticity of host 'ska01.ira.inaf.it (90.147.132.60)' can't be establishe
d.
ECDSA key fingerprint is SHA256:fUr/Gn3oGAvTZfGo3fUO9+HV+02VD7aDnn/slm1ABRA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ska01.ira.inaf.it,90.147.132.60' (ECDSA) to the list
 of known hosts.
skarc001@ska01.ira.inaf.it's password:
Warning: No xauth data; using fake authentication data for X11 forwarding.
Last login: Thu May  2 20:00:27 2019 from mambo.ira.inaf.it
-bash: warning: setlocale: LC_CTYPE: cannot change locale (UTF-8): No such file
or directory
[skarc001@ska01 ~]$ ls
data
[skarc001@ska01 ~]$ cd data
[skarc001@ska01 data]$ ls
ska_rc_demo_01.fits  ska_rc_demo_02.fits
[skarc001@ska01 data]$ ds9 ska_rc_demo_02.fits
Fontconfig warning: ignoring UTF-8: not a valid region tag
```



Login to computing element and analyze data

The Prototype Step by Step (4.3)



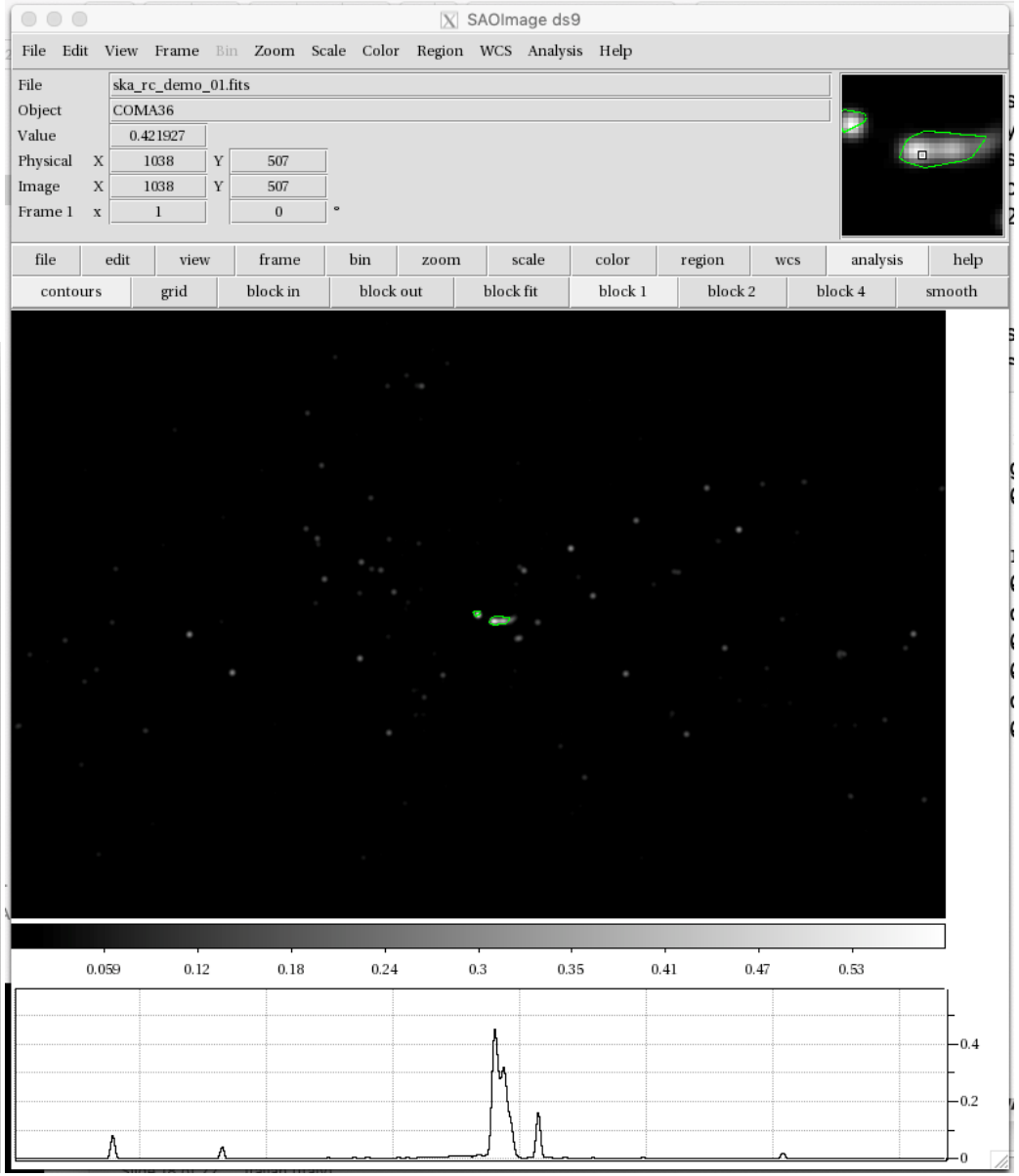


Send your ssh public keys to login without password

The Prototype Step by Step (4.3.1)

Login without password and analyze data

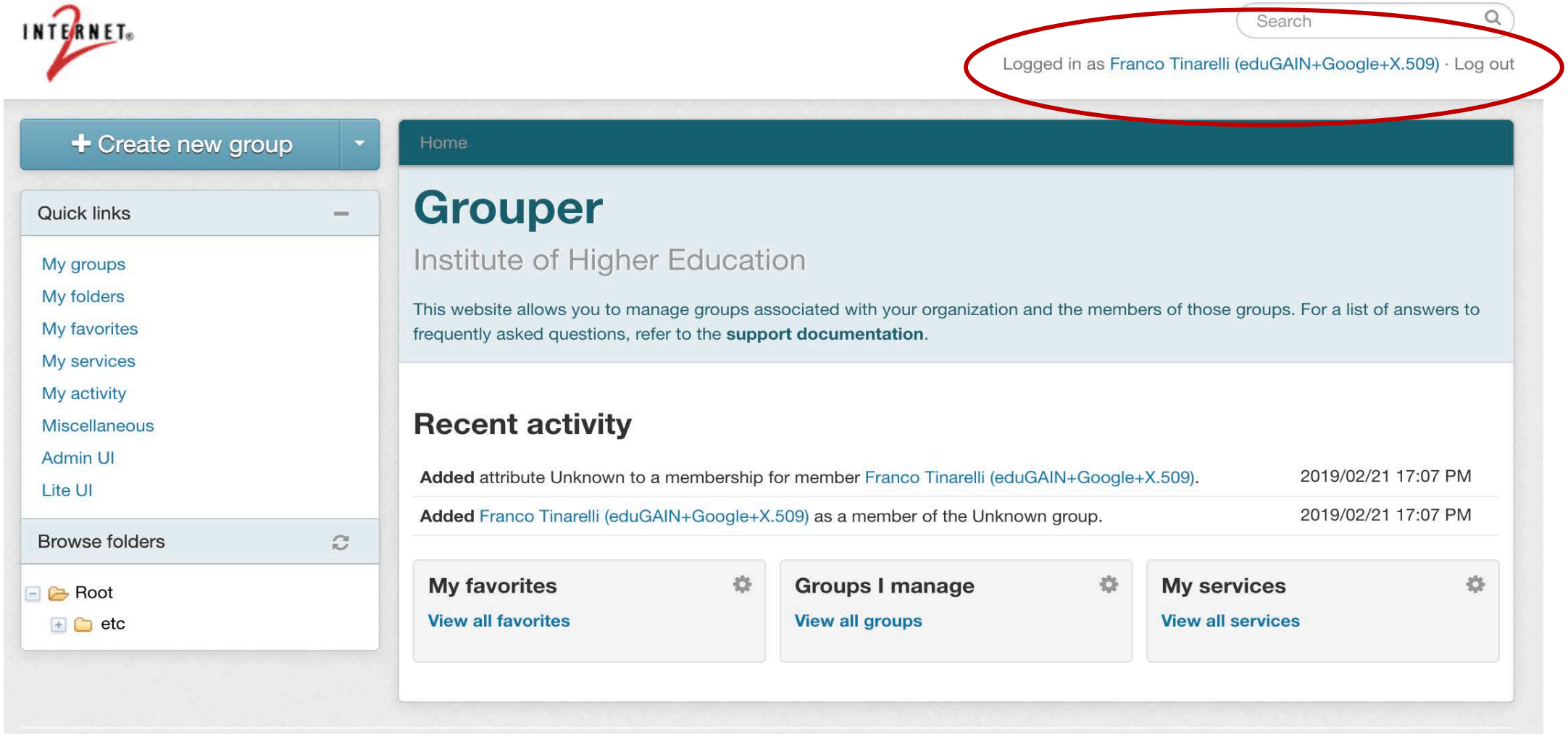
```
ftinarel — skarc004@ska01:~/data — ssh -Y skarc004@ska01.ira.inaf.it — 80×24
mambo:~ ftinarel$ ssh -Y skarc004@ska01.ira.inaf.it
Warning: No xauth data; using fake authentication data for X11 forwarding.
Last login: Fri May 31 18:55:13 2019 from mambo.ira.inaf.it
[skarc004@ska01 ~]$ ls -l
total 0
lrwxrwxrwx 1 skarc004 srcusers 23 May 31 18:48 data -> /data/ST_2022_1_00001_L
[skarc004@ska01 ~]$ ls data
ska_rc_demo_01.fits  ska_rc_demo_02.fits
[skarc004@ska01 ~]$ cd data
[skarc004@ska01 data]$ ls
ska_rc_demo_01.fits  ska_rc_demo_02.fits
[skarc004@ska01 data]$ ds9 ska_rc_demo_01.fits
```



RAP and Grouper at INAF IA2 Archive

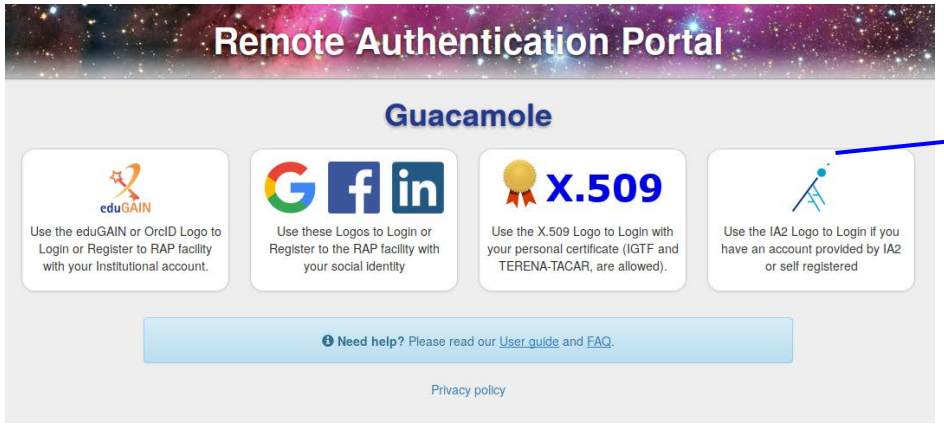
RAP use two modified grouper connectors (Sonia Zorba IA2 staff) to authenticate PI as grouper administrator to manage group memberships of archived data files.

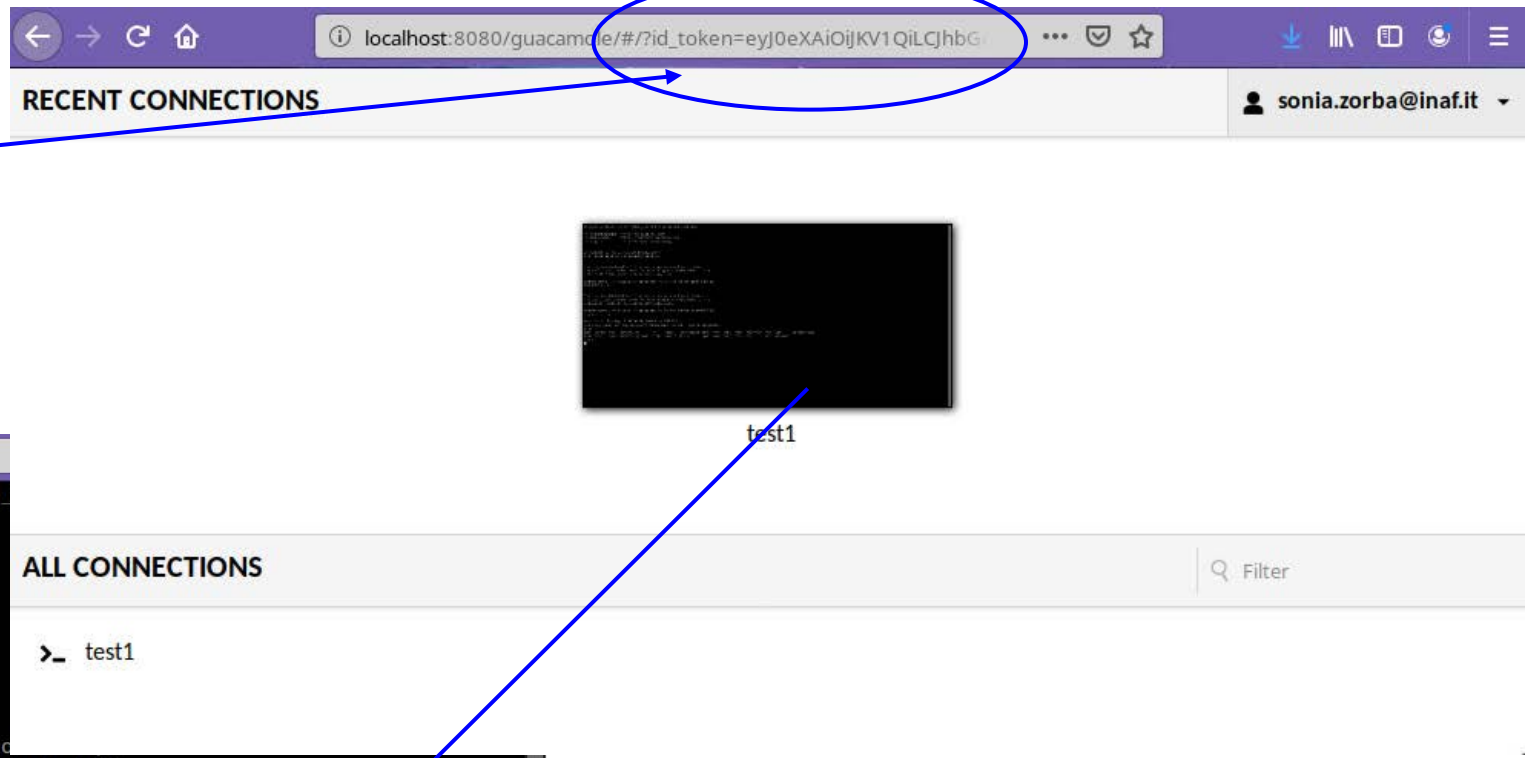
RAP and Grouper and the Account Linking

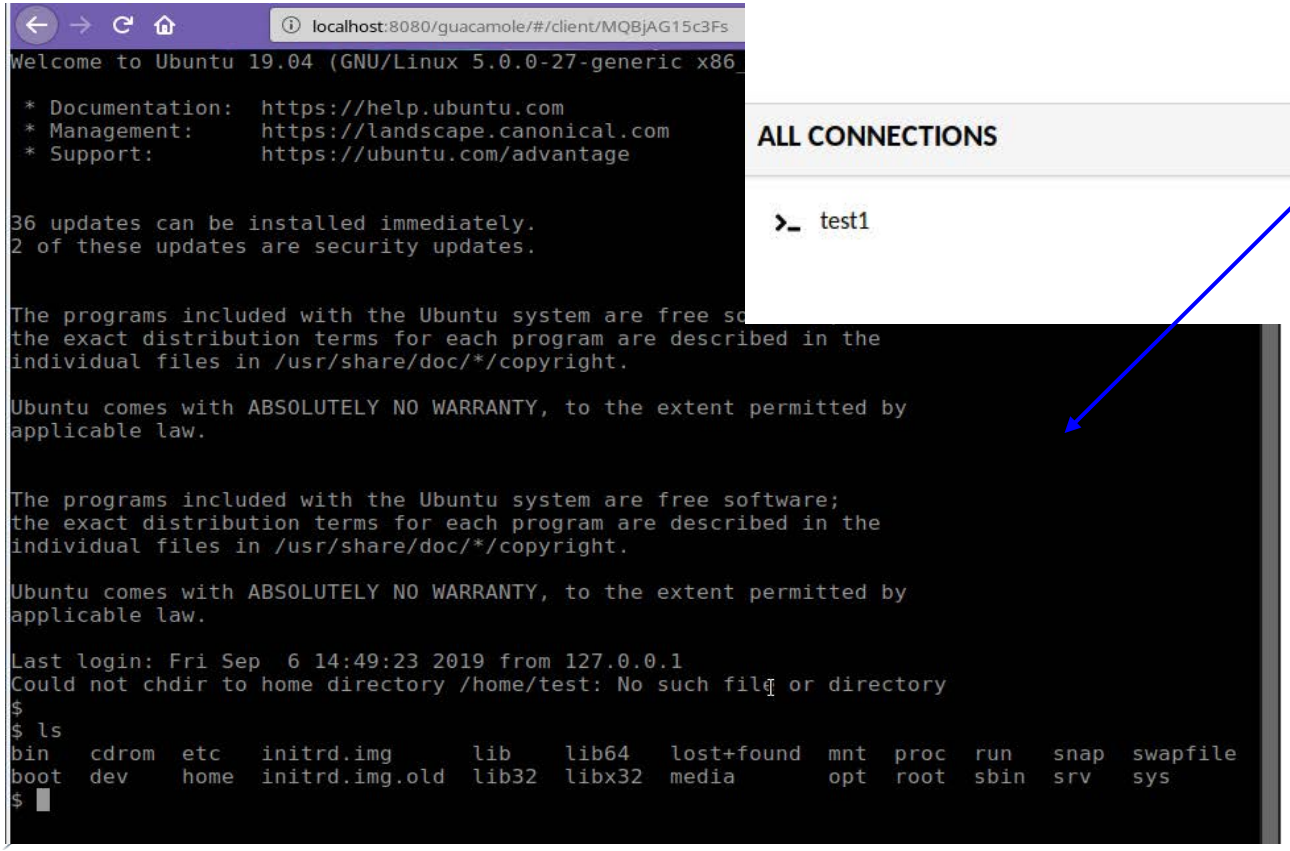


Using the two modified connectors, grouper receives the joined identities (Account Linking) from RAP.

RAP and Guacamole (courtesy of Sonia Zorba)







Web oriented connection using several protocols like ssh, VNC, telnet…..

Thanks for your attention!

Questions?