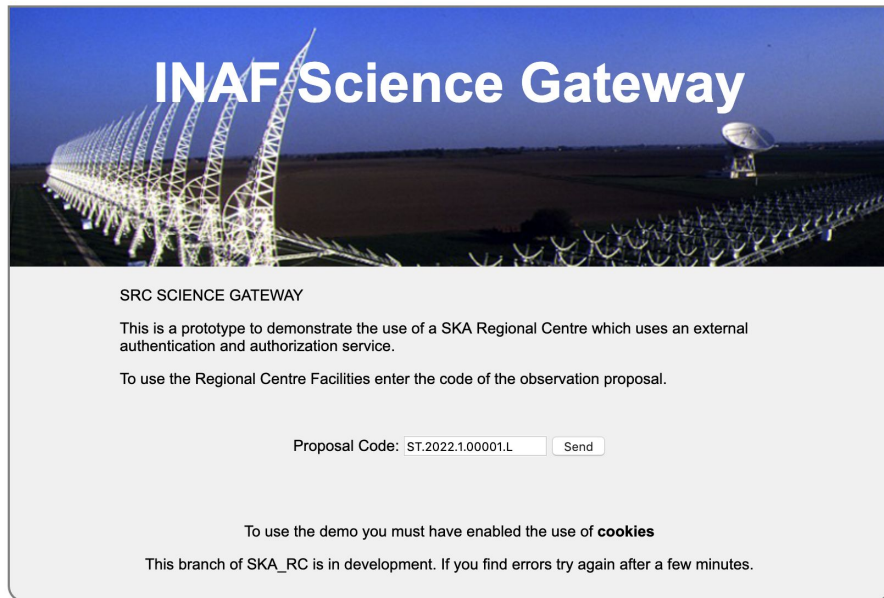


AENEAS Authentication and Authorization piloting activities

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

Prototype use case for SKA RC



INAF Science Gateway

SRC SCIENCE GATEWAY

This is a prototype to demonstrate the use of a SKA Regional Centre which uses an external authentication and authorization service.

To use the Regional Centre Facilities enter the code of the observation proposal.

Proposal Code:


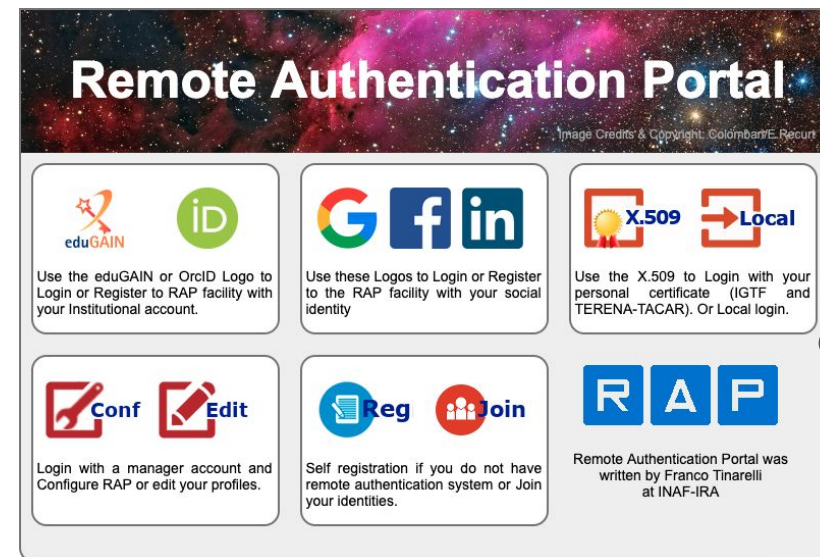
To use the demo you must have enabled the use of **cookies**

This branch of SKA_RC is in development. If you find errors try again after a few minutes.

Science Gateway Catalog













IN: proposalID


OUT: IVO-ID, Data_Center, files,
ivo://authority.org/path?groupID

Remote Authentication Portal

Image Credits & Copyright: Colombari/E. Recurt

  Use the eduGAIN or OrCID Logo to Login or Register to RAP facility with your Institutional account.	   Use these Logos to Login or Register to the RAP facility with your social identity	  Use the X.509 to Login with your personal certificate (IGTF and TERENA-TACAR). Or Local login.
  Login with a manager account and Configure RAP or edit your profiles.	  Self registration if you do not have remote authentication system or Join your identities.	 Remote Authentication Portal was written by Franco Tinarelli at INAF-IRA



IN: Authentication

OUT: User Unique ID

Data Center (Archive+Computation)


Token exchange

Data access and computation

Grouper/GMS

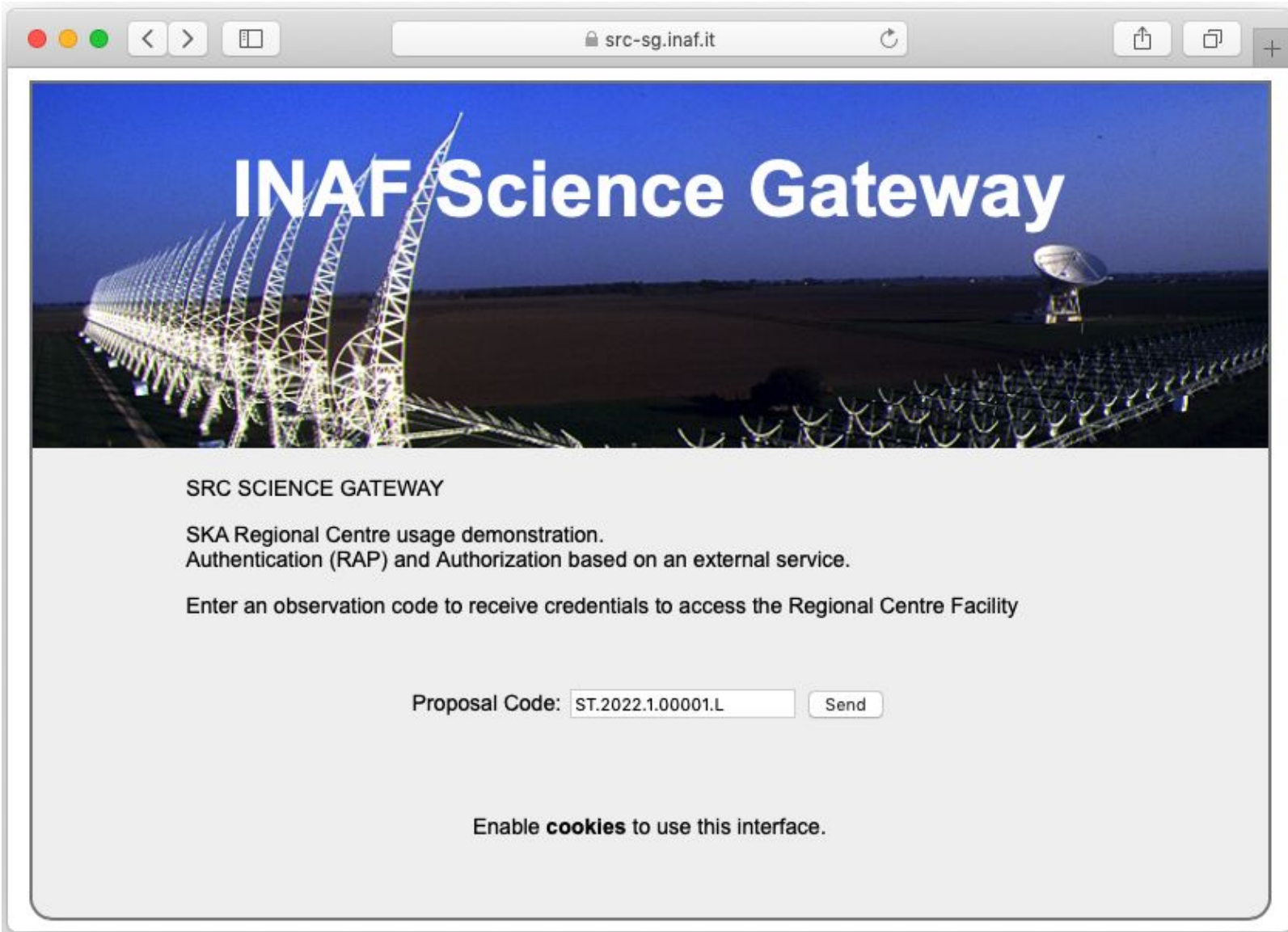
IN: groupID, user_unique_ID

OUT: authorization

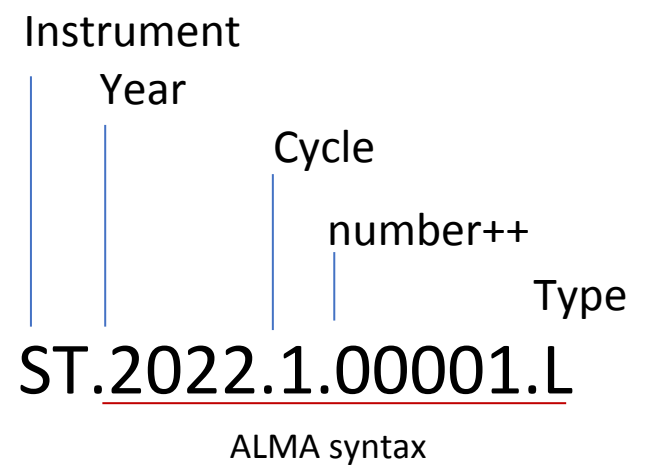


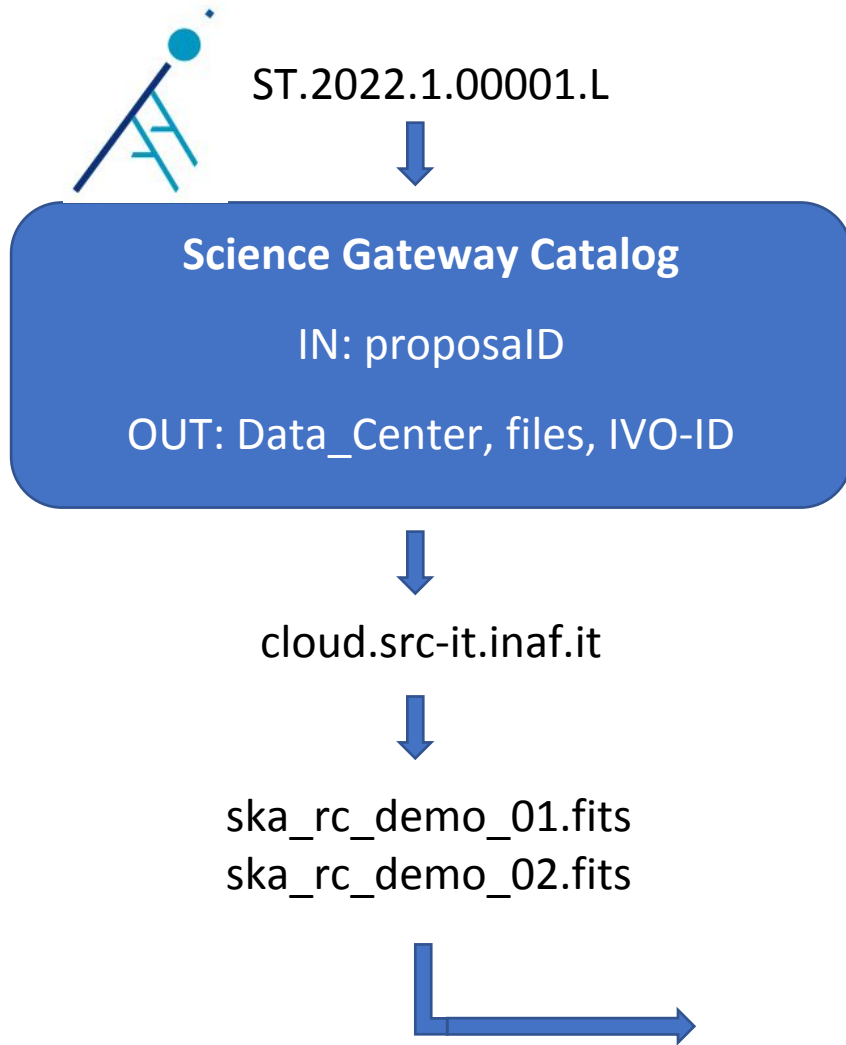



Actors: The Science Gateway



- 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 a single observational project
- If the syntax of the proposal_ID become a standard, it could serve more observational project





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 resolve the service URL to call for authN and authZ purposes
- The group ID of the proposal dataset belongs to

`ivo://authority.org/path?groupID`

`(ivo://auth.ska.org/https://sso.ia2.inaf.it?ST_2022_1_00001_L)`





Actors: The Remote Authentication Portal (RAP)

Remote Authentication Portal

Image Credits & Copyright: Colómbani/E.Recurr

- Use the eduGAIN or OrCID Logo to Login or Register to RAP facility with your Institutional account.
- Use these Logos to Login or Register to the RAP facility with your social identity
- Use the X.509 to Login with your personal certificate (IGTF and TERENA-TACAR). Or Local login.
- Login with a manager account and Configure RAP or edit your profiles.
- Self registration if you do not have remote authentication system or Join your identities.
- Remote Authentication Portal was written by Franco Tinarelli at INAF-IRA

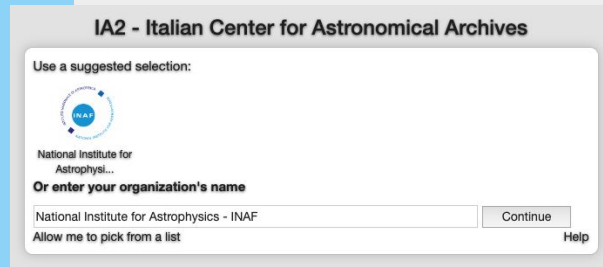
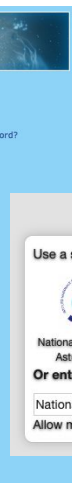
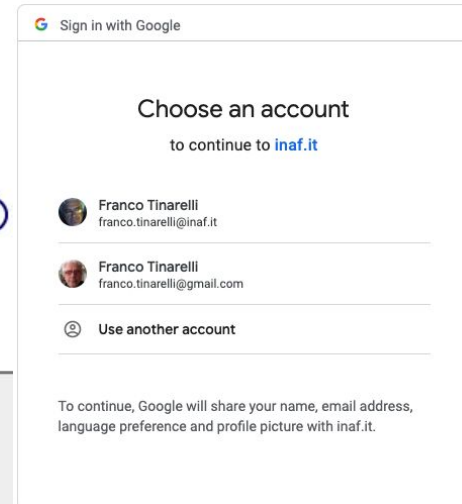
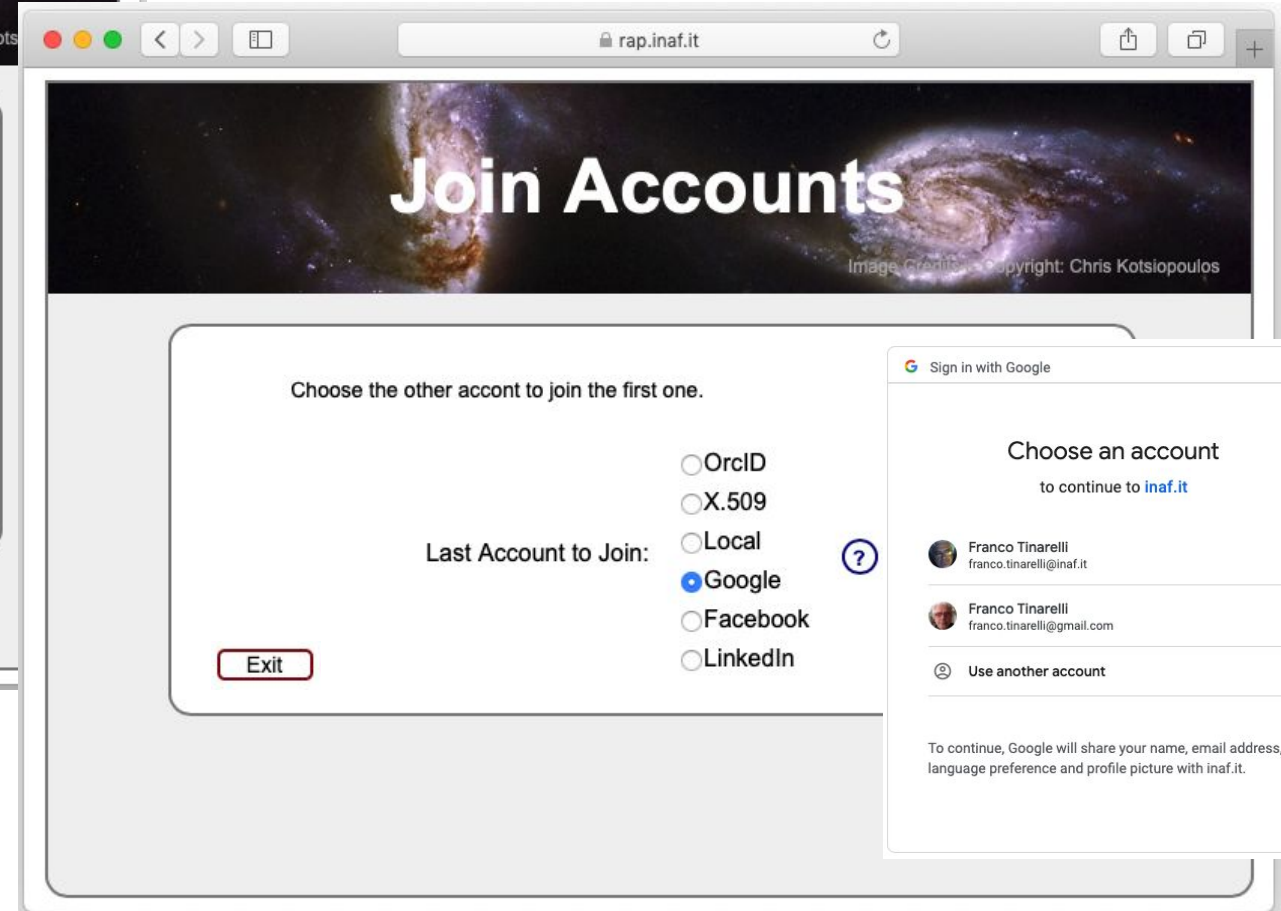
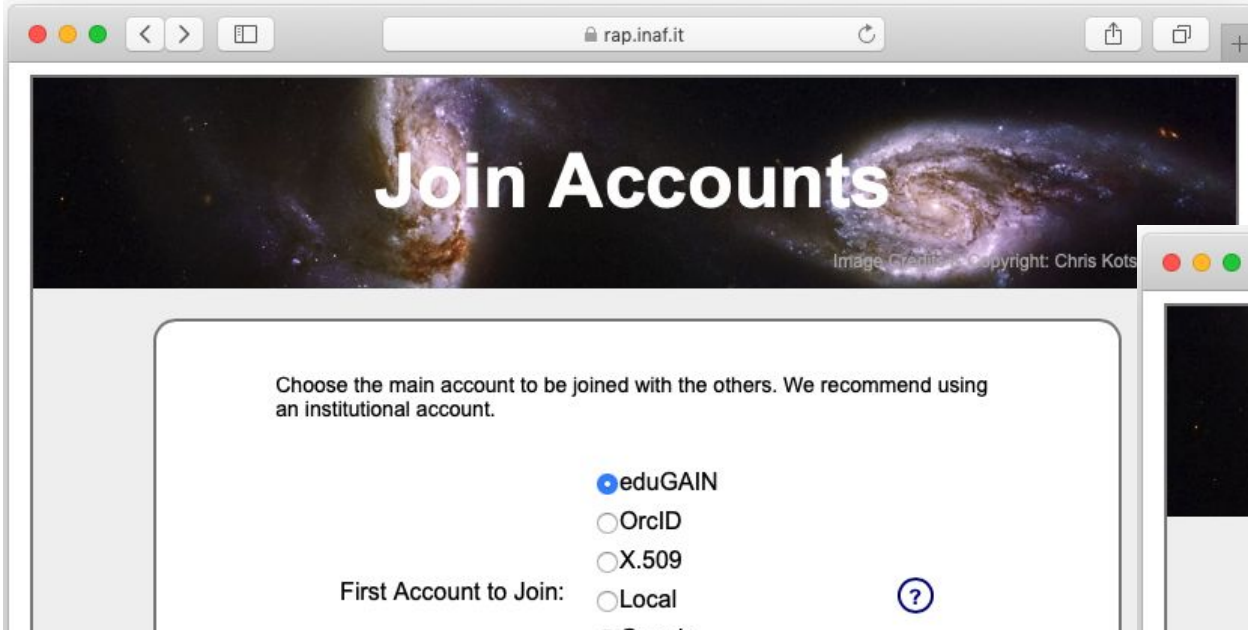
- RAP is an Authentication system built by INAF capable to handle multiple accounts for web application usage
- Born as a SKA Pre-construction phase component - a joint venture between Radio Astronomical Institute (IRA) and Italian Astronomical Archives (IA2)
- The first RAP prototype has been presented 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)**

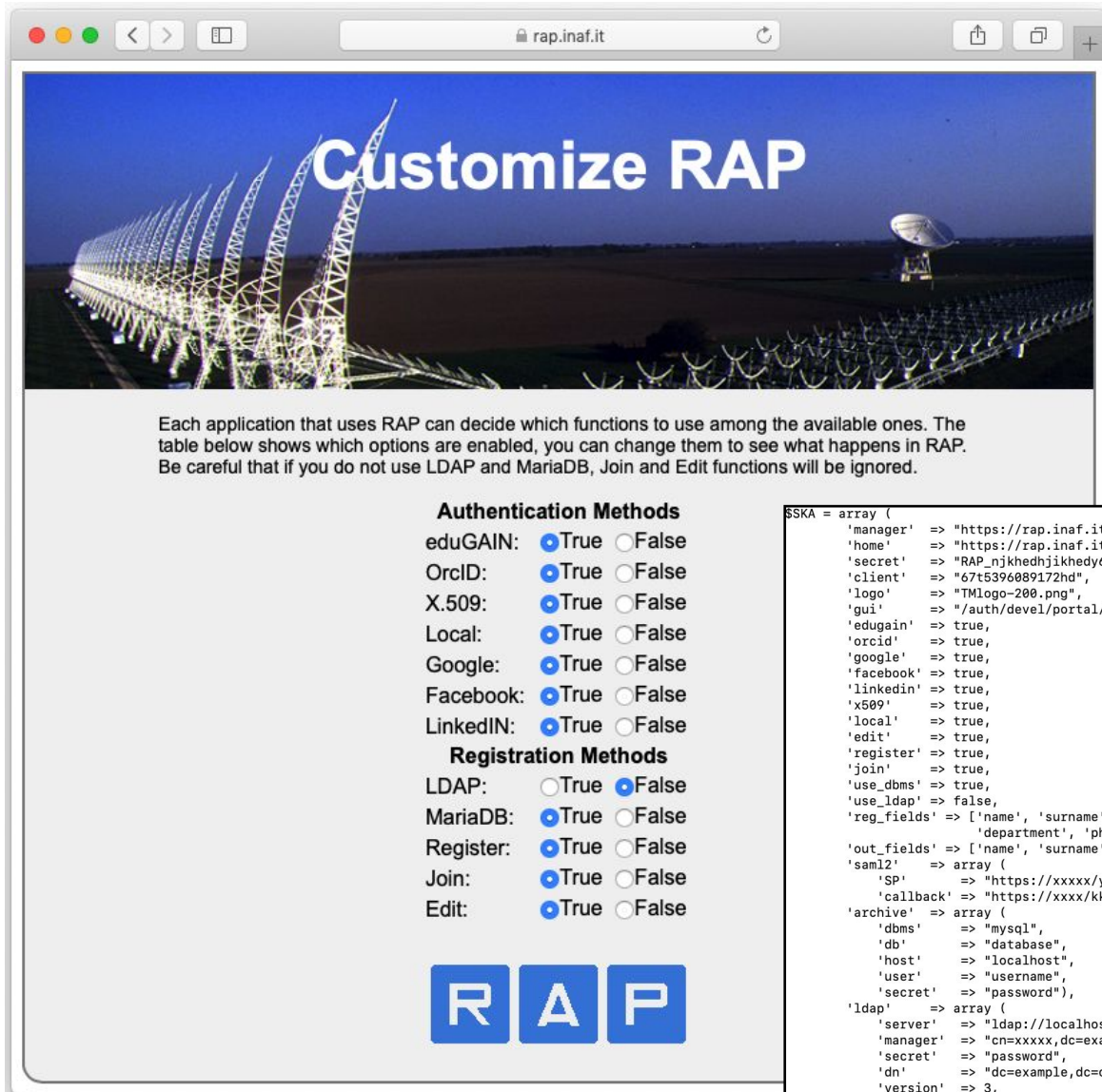
(Use the link <https://rap.inaf.it/Services/RAP> to test a fully functioning demonstration.)



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 institutional account as the reference one to join against to.





Each application that uses RAP can decide which functions to use among the available ones. The table below shows which options are enabled, you can change them to see what happens in RAP. Be careful that if you do not use LDAP and MariaDB, Join and Edit functions will be ignored.

Authentication Methods	
eduGAIN:	<input checked="" type="radio"/> True <input type="radio"/> False
OrcID:	<input checked="" type="radio"/> True <input type="radio"/> False
X.509:	<input checked="" type="radio"/> True <input type="radio"/> False
Local:	<input checked="" type="radio"/> True <input type="radio"/> False
Google:	<input checked="" type="radio"/> True <input type="radio"/> False
Facebook:	<input checked="" type="radio"/> True <input type="radio"/> False
LinkedIN:	<input checked="" type="radio"/> True <input type="radio"/> False
Registration Methods	
LDAP:	<input type="radio"/> True <input checked="" type="radio"/> False
MariaDB:	<input checked="" type="radio"/> True <input type="radio"/> False
Register:	<input checked="" type="radio"/> True <input type="radio"/> False
Join:	<input checked="" type="radio"/> True <input type="radio"/> False
Edit:	<input checked="" type="radio"/> True <input type="radio"/> False

RAP

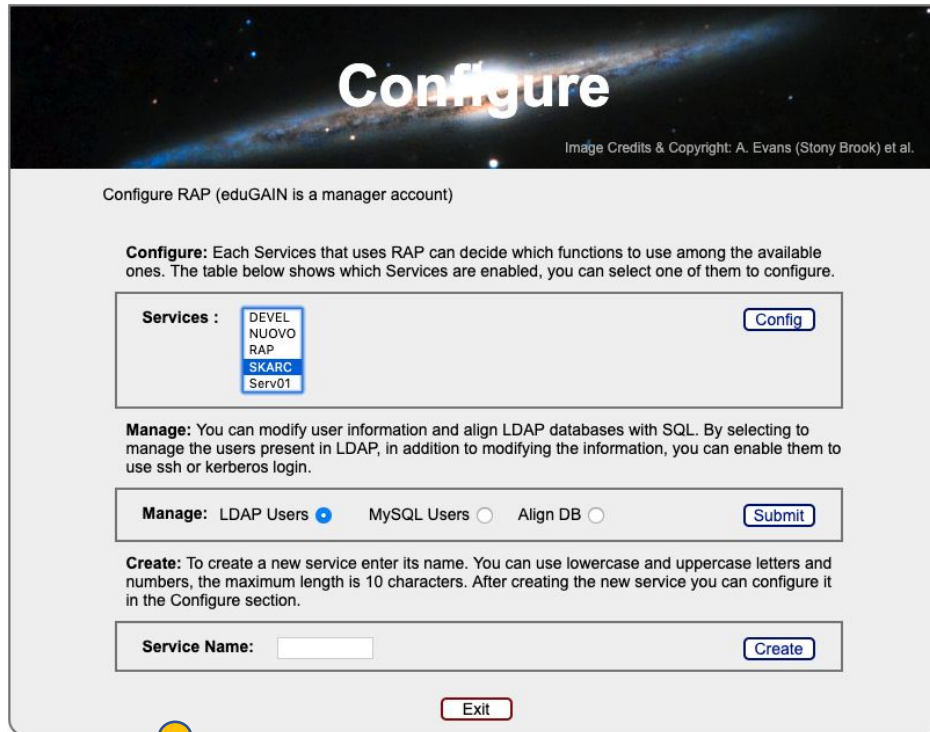
```

$SKA = array (
  'manager' => "https://rap.inaf.it/xxxxx/Kkkkkk.php",
  'home' => "https://rap.inaf.it/xxxxx",
  'secret' => "RAP_njkhednjikhedy60t5667536tiugedgh",
  'client' => "67t5396089172hd",
  'logo' => "TLogo-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', 'uniqueid'],
  '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=xxxx,dc=example,dc=org",
    'secret' => "password",
    'dn' => "dc=example,dc=org",
    'version' => 3,
    'tls' => true));
  
```

Proxy between applications and identity providers or local registration

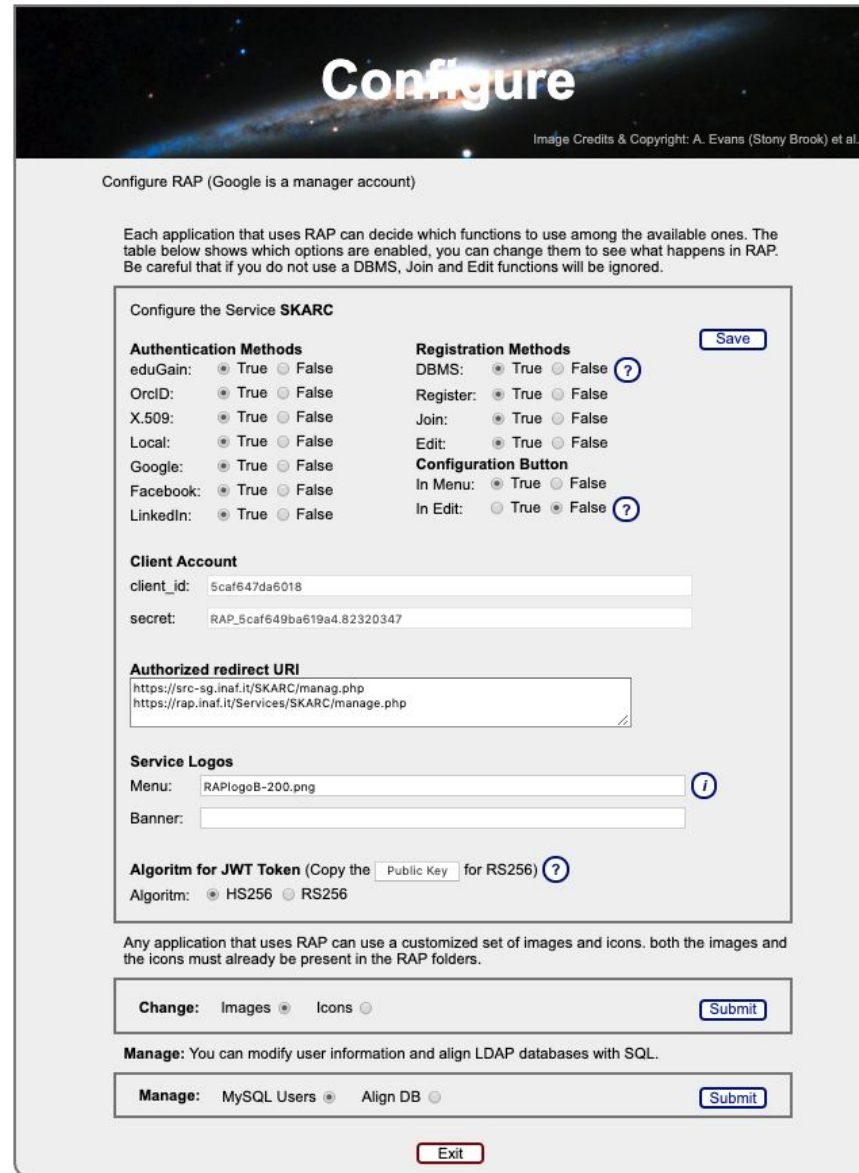
It can be customized from applications (through configuration command or editing file):

- 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
- SQL Servers for user registration at first login (required for account linking) are supported
- 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



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 Algorithm 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;

The Prototype Step by Step (3)

Select the actions to manage
your data

src-sg.inaf.it

INAF Science Gateway User Data

LOGIN WITH **Google** (franco.tinarelli@gmail.com)

JOINED IDENTITIES:

Facebook (franco.tinarelli@alice.it); **eduGAIN** (f.tinarelli@ira.inaf.it);

PROPOSAL ST.2022.1.00001.L (Ownership: Full)

ACTIONS:

- Download Experiment Files
- Receive Account to Analyse Experiment files
- Send ssh Public Key to receive Username to Analyse Experiment files

Move Experiment Files to another SRC

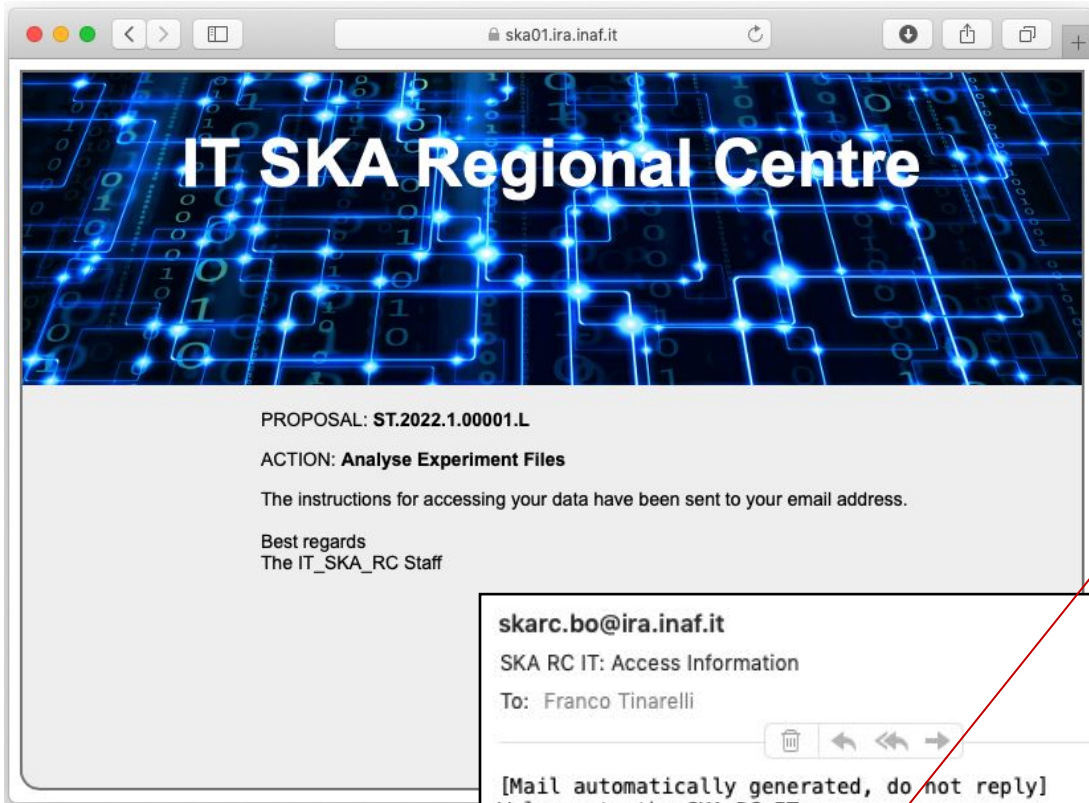
Send

The Prototype Step by Step (4.1)

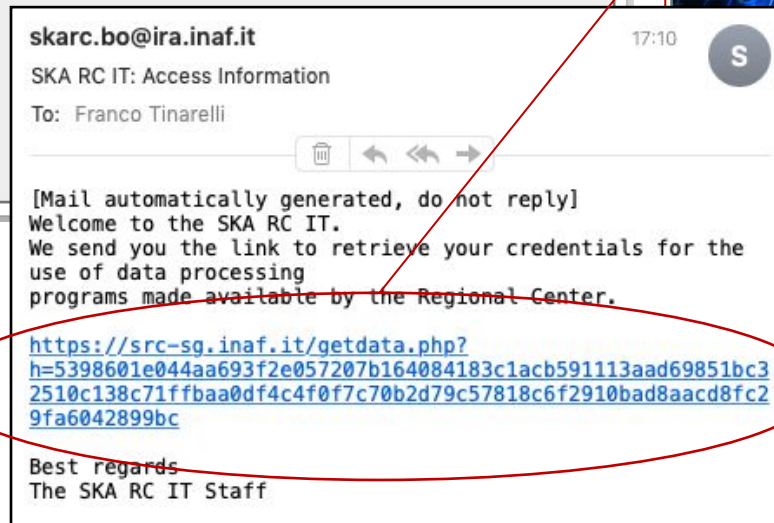
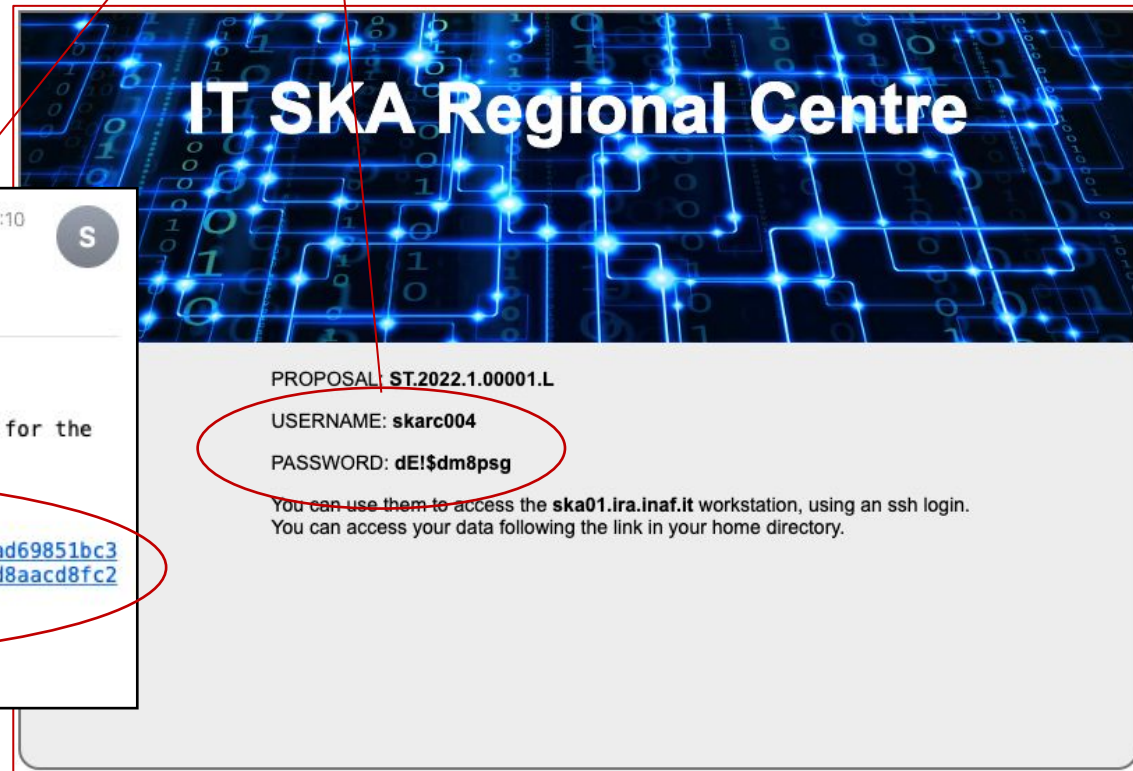
Download experiment files

The screenshot shows a web browser window with the address bar displaying 'ska01.ira.inaf.it'. The main content area features a blue background with a circuit-like pattern and the text 'IT SKA Regional'. Below this, the text reads: 'PROPOSAL: ST.2022.1.00001.L' and 'ACTION: Download Experiment Files'. Two download links are listed: 'ska_rc_demo_01.fits, Size: 8527680 byte' and 'ska_rc_demo_02.fits, Size: 1126080 byte', each with a 'Download' button. A red oval highlights these two links. A 'Downloads' panel is open on the right side of the browser, showing two files: 'ska_rc_demo_02.fits' (1,1 MB) and 'ska_rc_demo_01.fits' (8,5 MB). A red line connects the text 'Download experiment files' to the highlighted download links.

The Prototype Step by Step (4.2)



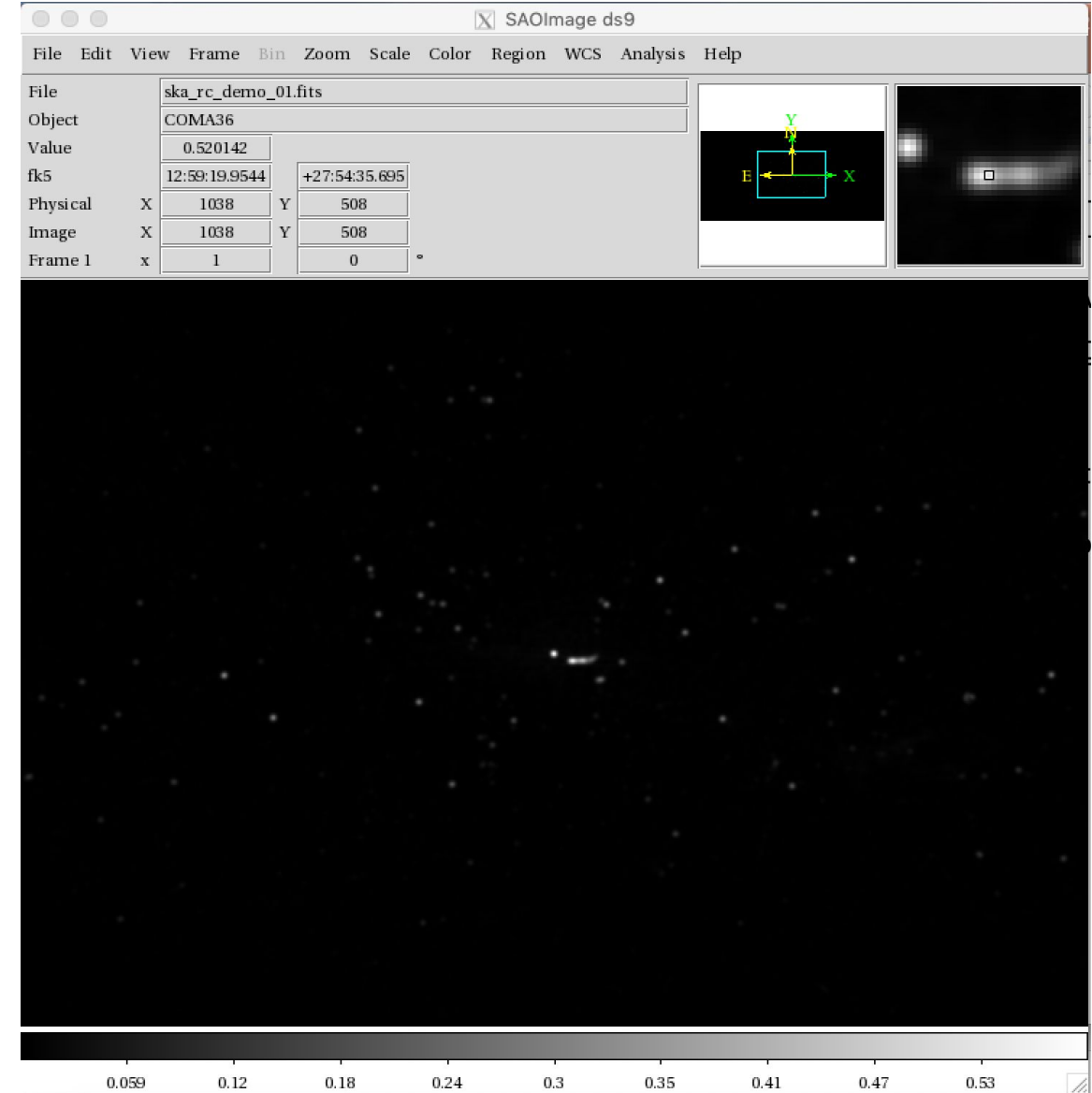
Obtain an account to analyze your data



The Prototype Step by Step (4.2.1)

```

bertocco — skarc001@ska01:~/data — ssh -XY skarc001@ska01.ira.inaf.it — 80x24
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 established.
ECDSA key fingerprint is SHA256:fUr/Gn3oGAvTZfGo3fU09+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
  
```

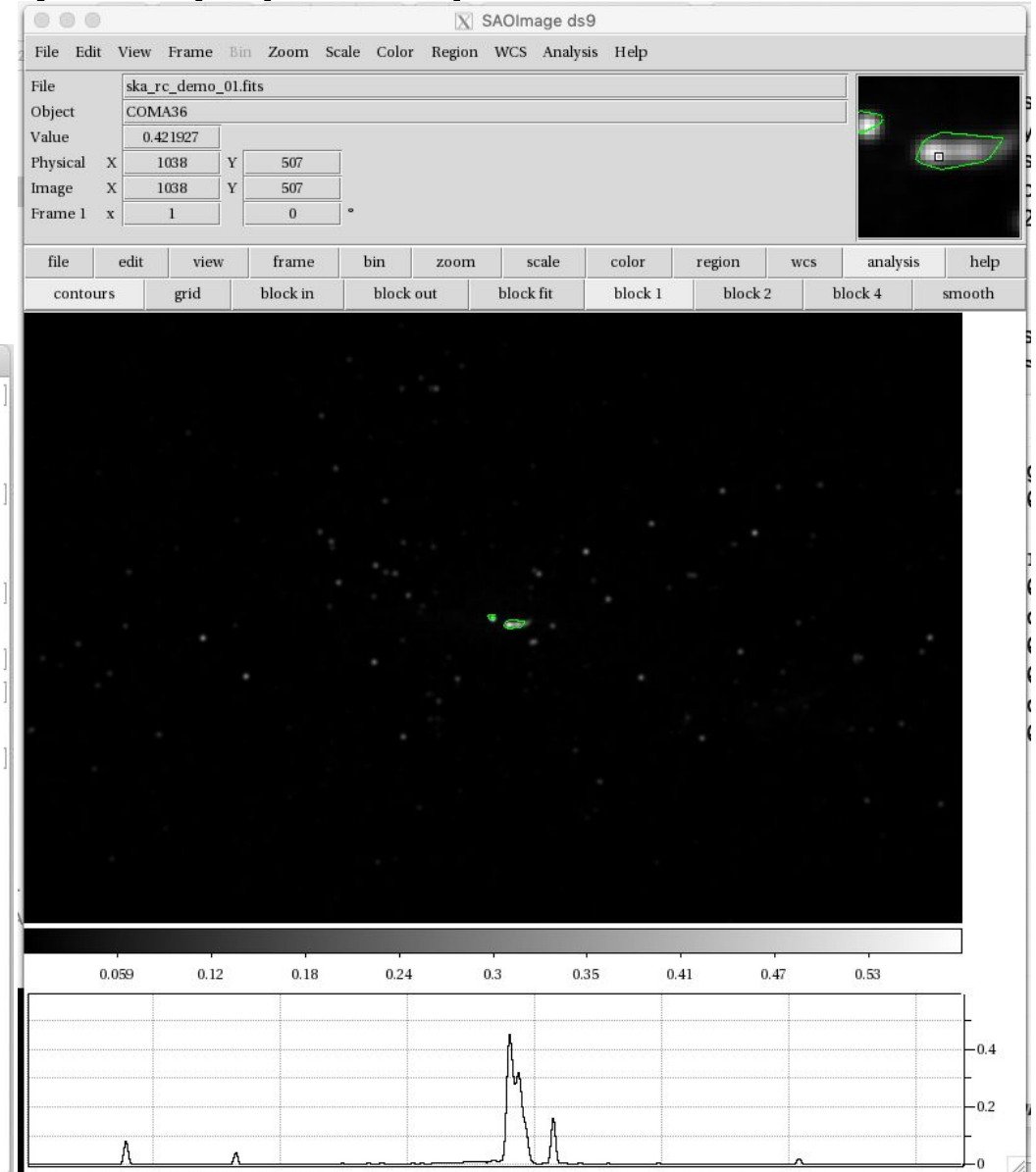


Login to computing element
 and analyze data

The Prototype Step by Step (4.3.1)

Login without password and analyze data

```
ftinare1 ~ skarc004@ska01:~/data — ssh -Y skarc004@ska01.ira.inaf.it — 80x24
mambo:~ ftinare1$ 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
```



Remote Authentication Portal

Image Credits & Copyright: Colombari/E.Recurr

Login to Grouper



Use the eduGAIN Logo to Login or Register to the RAP facility if you belong to an eduGAIN IdP.



Use these Logos to Login or Register to the RAP facility with your social identity



Use the X.509 Logo to Login with your personal certificate (IGTF and TERENA-TACAR, are allowed).



Use the IA2 Logo to Login if you have an account provided by IA2 or self registered

 **Need help?** Please read our [User guide](#) and [FAQ](#).

[Privacy policy](#)

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



Search

Logged in as Franco Tinarelli (eduGAIN+Google+X.509) · Log out

+ Create new group

Quick links

- My groups
- My folders
- My favorites
- My services
- My activity
- Miscellaneous
- Admin UI
- Lite UI

Browse folders

- Root
- etc

Home

Grouper

Institute of Higher Education

This website allows you to manage groups associated with your organization and the members of those groups. For a list of answers to frequently asked questions, refer to the [support documentation](#).

Recent activity

Added attribute Unknown to a membership for member Franco Tinarelli (eduGAIN+Google+X.509) .	2019/02/21 17:07 PM
Added Franco Tinarelli (eduGAIN+Google+X.509) as a member of the Unknown group.	2019/02/21 17:07 PM

My favorites [View all favorites](#)

Groups I manage [View all groups](#)

My services [View all services](#)

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





RAP and Guacamole (courtesy of Sonia Zorba)

```

localhost:8080/guacamole/#/client/MQBjAG15c3Fs
Welcome to Ubuntu 19.04 (GNU/Linux 5.0.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

36 updates can be installed immediately.
2 of these updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Fri Sep  6 14:49:23 2019 from 127.0.0.1
Could not chdir to home directory /home/test: No such file or directory
$
$ ls
bin   cdrom  etc     initrd.img       lib     lib64   lost+found  mnt  proc  run  snap  swapfile
boot  dev    home   initrd.img.old  lib32  libx32  media       opt  root  sbin  srv   sys
$
  
```

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



Thanks for your attention!

Questions?