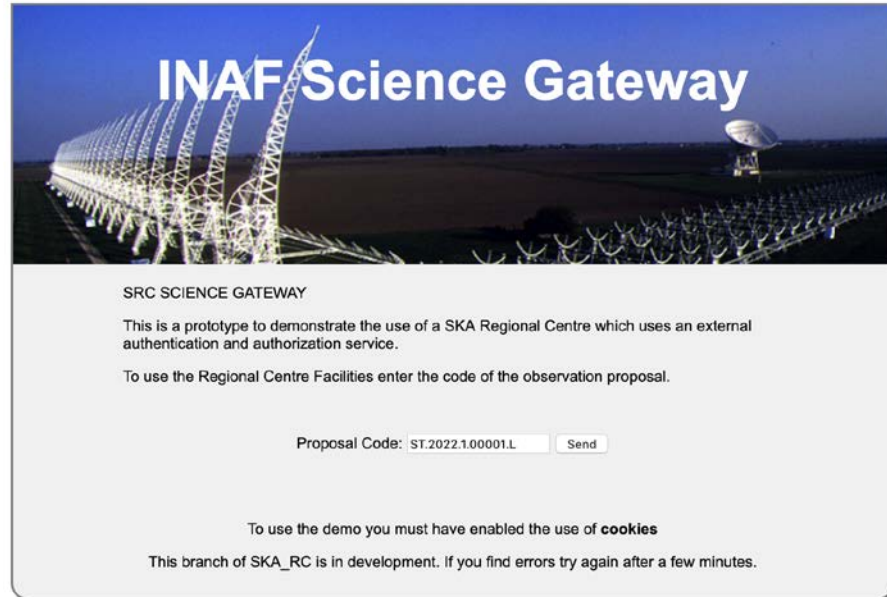


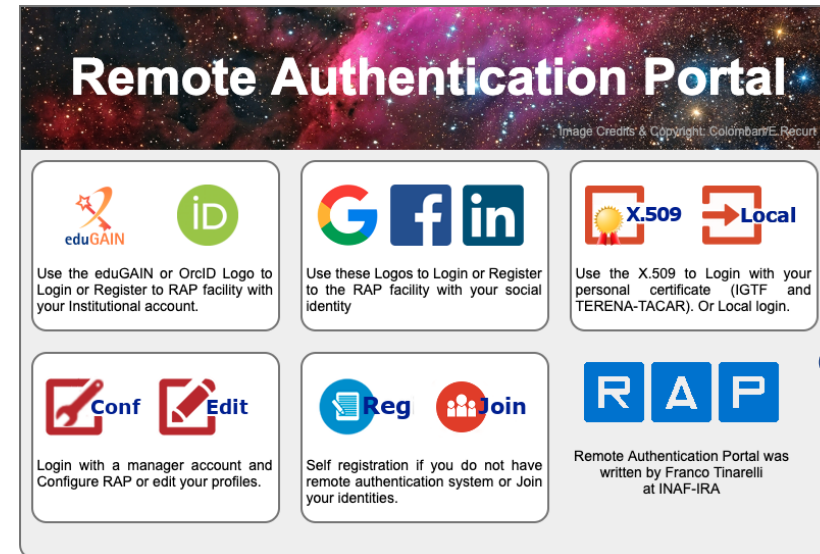
# Science Gateway Prototype

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

# Prototype use case for SKA RC



**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



# 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

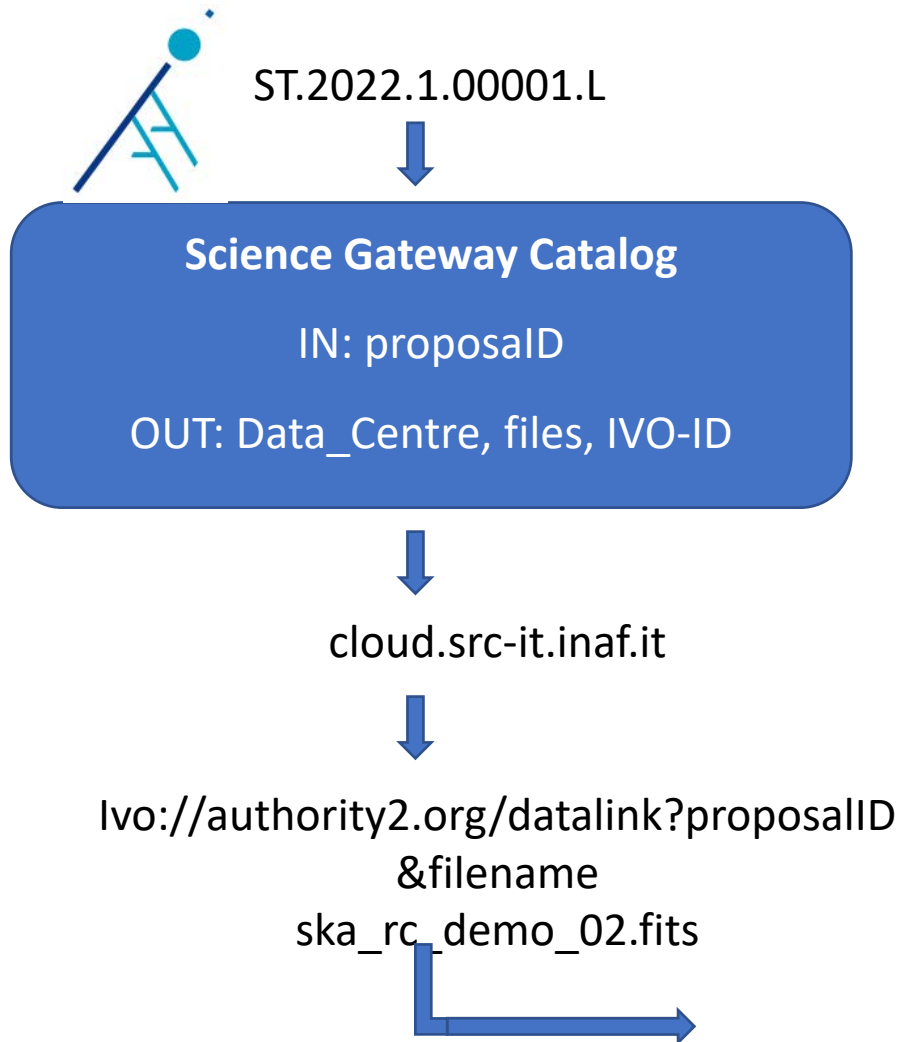
ST.2022.1.00001.L

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

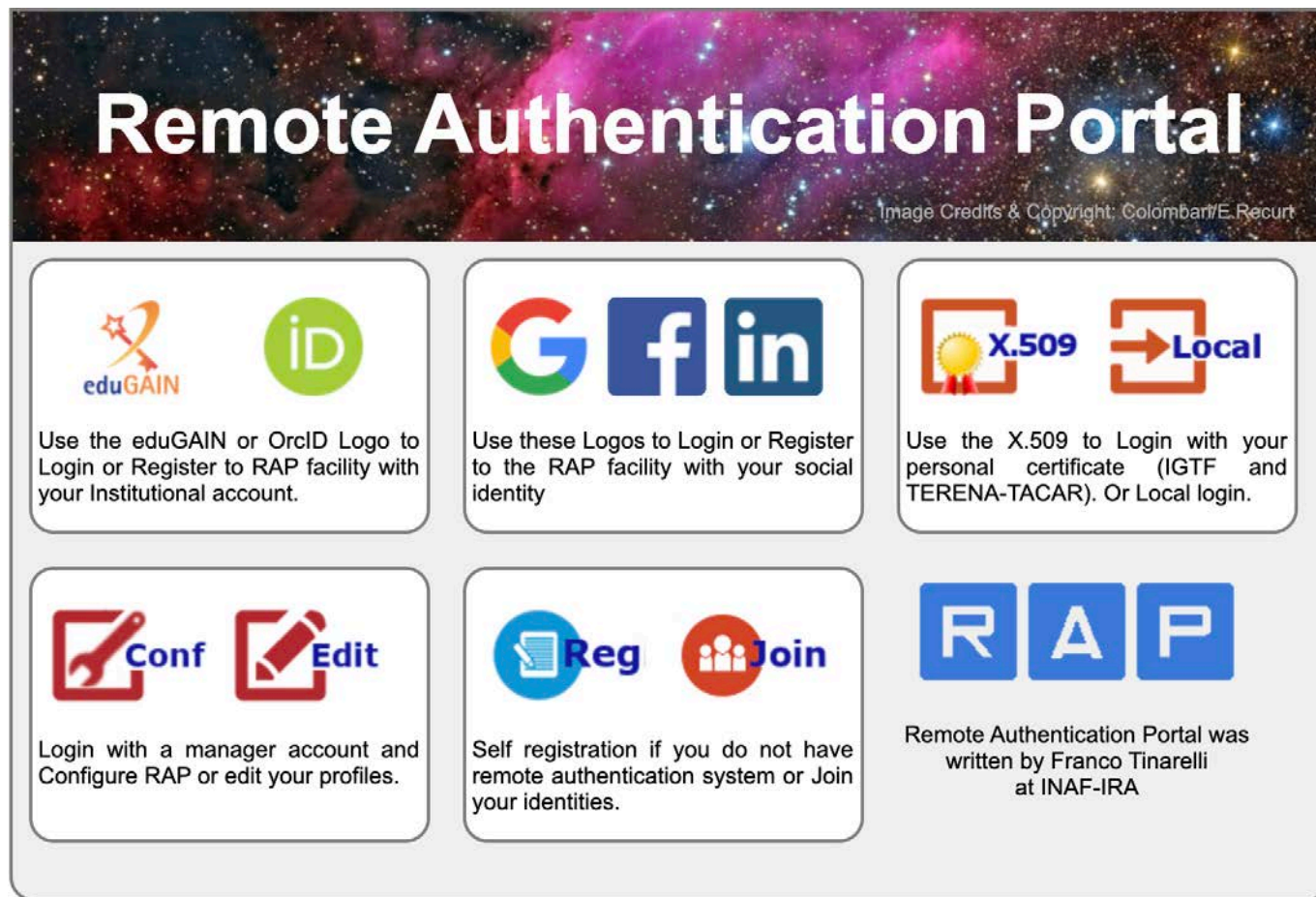
ivo://authority.org/path?groupID  
(ivo://auth.ska.org/grouper?ST\_2022\_1\_00001\_L)







# 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.



Choose the main account to be joined with the others. We recommend using an institutional account.

☒ eduGAIN

☐ OrcID

☐ X.509

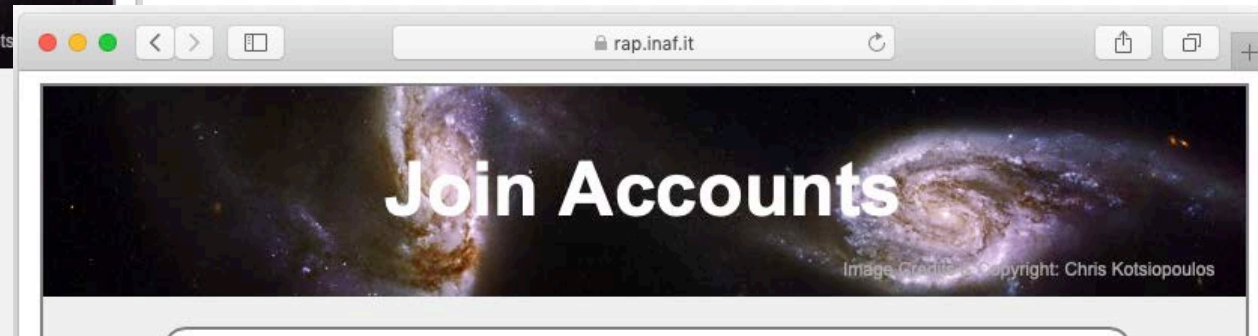
☐ Local

☐ Google

☐ Facebook

☐ LinkedIn

First Account to Join:



Choose the other acctont to join the first one.

☐ OrcID

☐ X.509

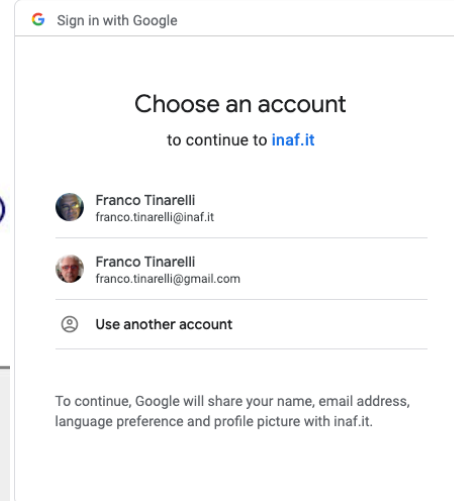
☐ Local

☒ Google

☐ Facebook

☐ LinkedIn

Last Account to Join:



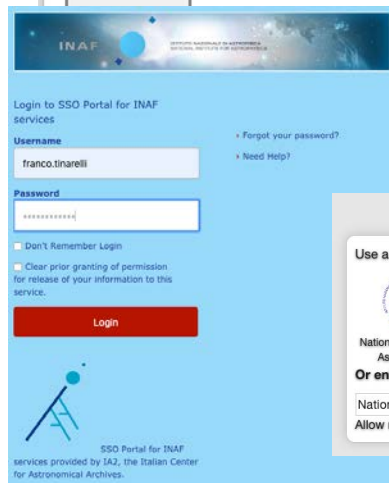
Choose an account  
to continue to [inaf.it](https://rap.inaf.it)

Franco Tinarelli  
franco.tinarelli@inaf.it

Franco Tinarelli  
franco.tinarelli@gmail.com

Use another account

To continue, Google will share your name, email address,  
language preference and profile picture with inaf.it.



IA2 - Italian Center for Astronomical Archives

Use a suggested selection:



National Institute for  
Astrophys...

Or enter your organization's name

National Institute for Astrophysics - INAF

Continue

Allow me to pick from a list

Help





# Actors: RAP and the DEMO Customization

Customize RAP

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: ☒ True ☐ False  
 OrCID: ☒ True ☐ False  
 X.509: ☒ True ☐ False  
 Local: ☒ True ☐ False  
 Google: ☒ True ☐ False  
 Facebook: ☒ True ☐ False  
 LinkedIn: ☒ True ☐ False

**Registration Methods**

LDAP: ☐ True ☒ False  
 MariaDB: ☒ True ☐ False  
 Register: ☒ True ☐ False  
 Join: ☒ True ☐ False  
 Edit: ☒ True ☐ False

RAP

```

$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', '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));
  
```

**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





## 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;





# Actors: The Science Gateway GMS

ST\_2022\_1\_00001\_L / 10001



53330313931303232f7ce4ea1@rap.inaf.it



**Grouper/GMS**

IN: groupID, user\_unique\_ID  
OUT: authorization



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.

LOGIN WITH **Google** (sara.bertocco@gmail.com)

JOINED IDENTITIES:

**eduGAIN** (sara.bertocco@inaf.it);

PROPOSAL ST.2022.1.00003.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



# Actors: The Data Centre

Token exchange with Science Gateway

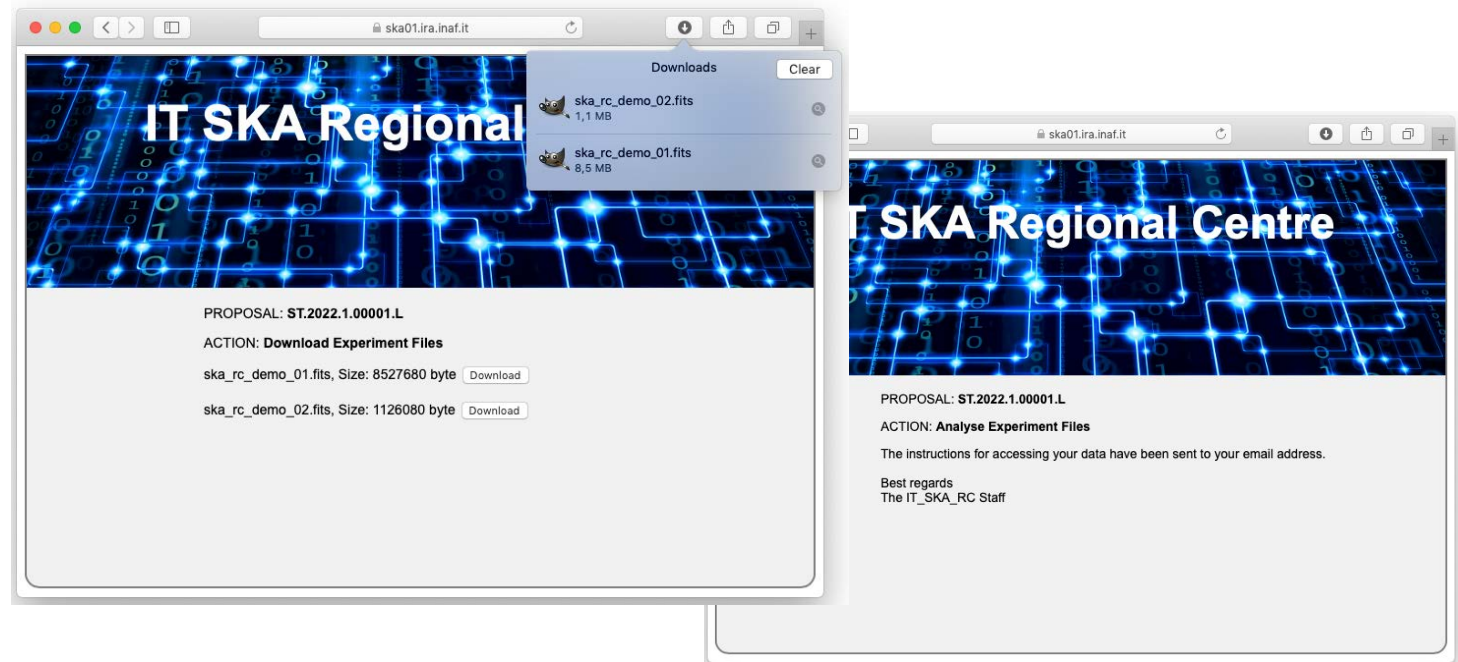


**Data Centre (Archive+Computation)**  
 Token exchange  
 Data access and computation



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

src-sg.inaf.it

## INAF Science Gateway

SRC SCIENCE GATEWAY

SKA Regional Centre usage demonstration.  
Authentication (RAP) and Authorization based on an external service.

Enter an observation code to receive credentials to access the Regional Centre Facility

Proposal Code:













Enable **cookies** to use this interface.



Authenticate Yourself

## Remote Authentication Portal

Image Credits & Copyright: Colómbart/E.Recurt

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

# 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)

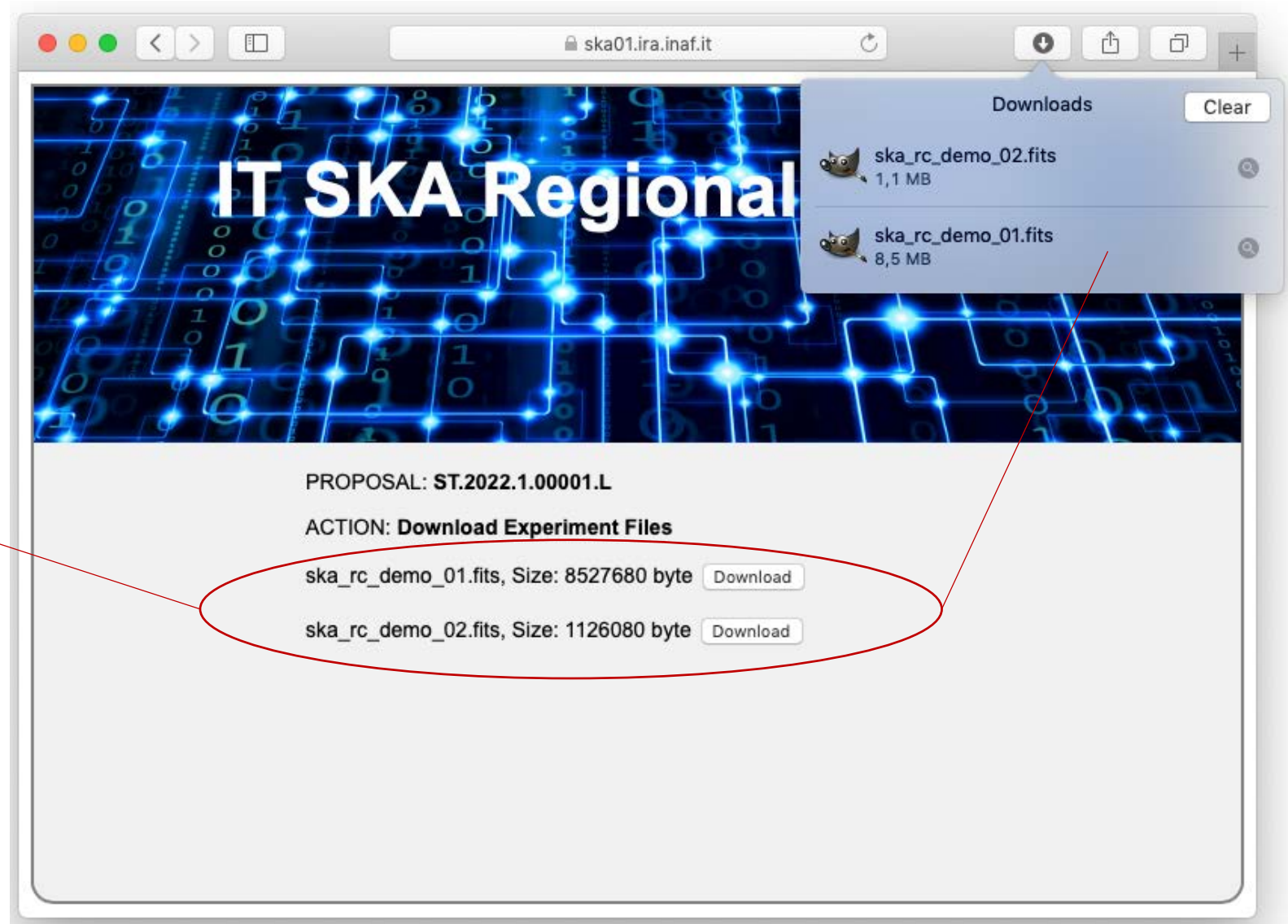
ACTIONS:

- ☐ 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

# The Prototype Step by Step (4.1)

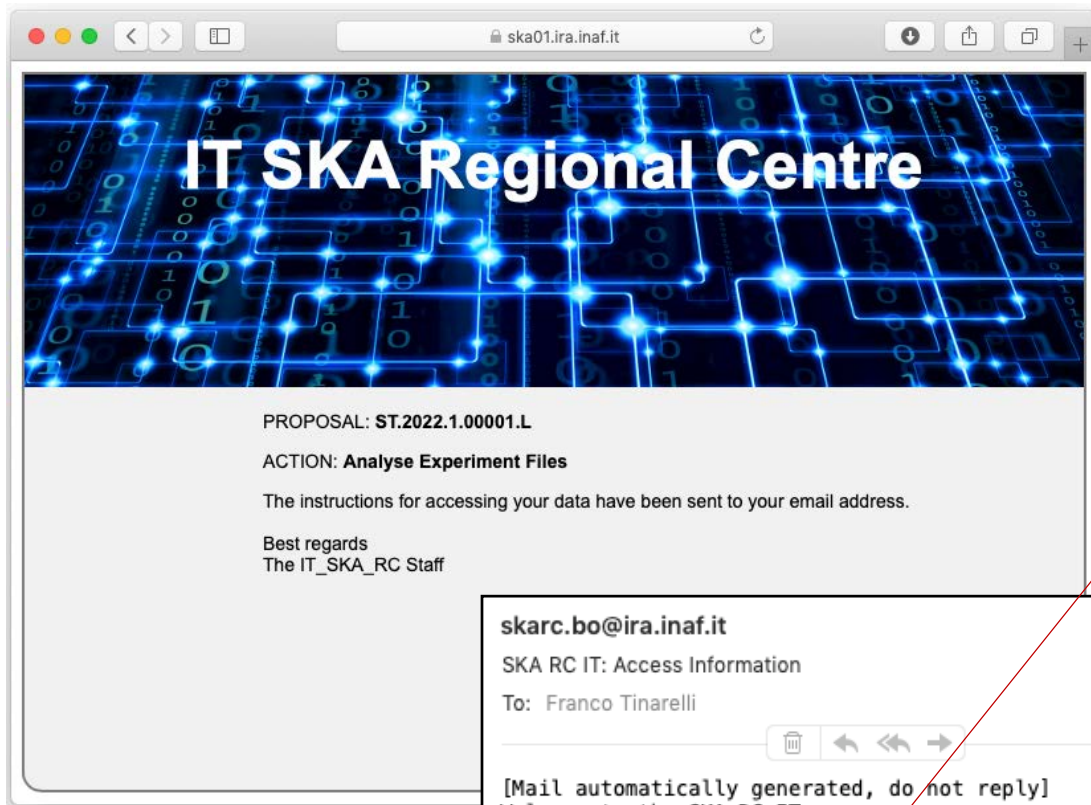
Download experiment files



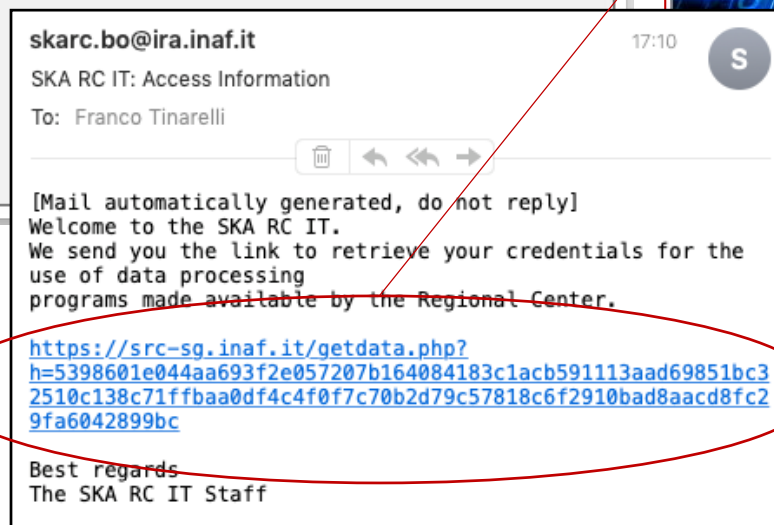
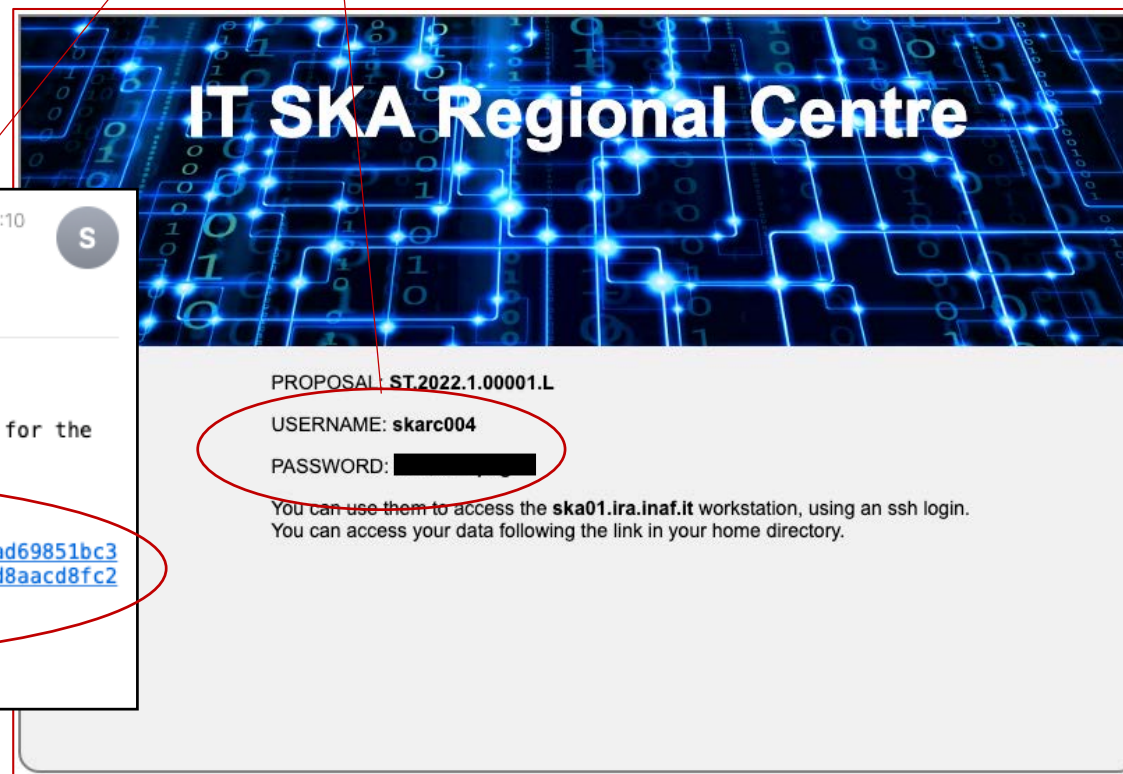




# The Prototype Step by Step (4.2)



Obtain an account to analyze your data

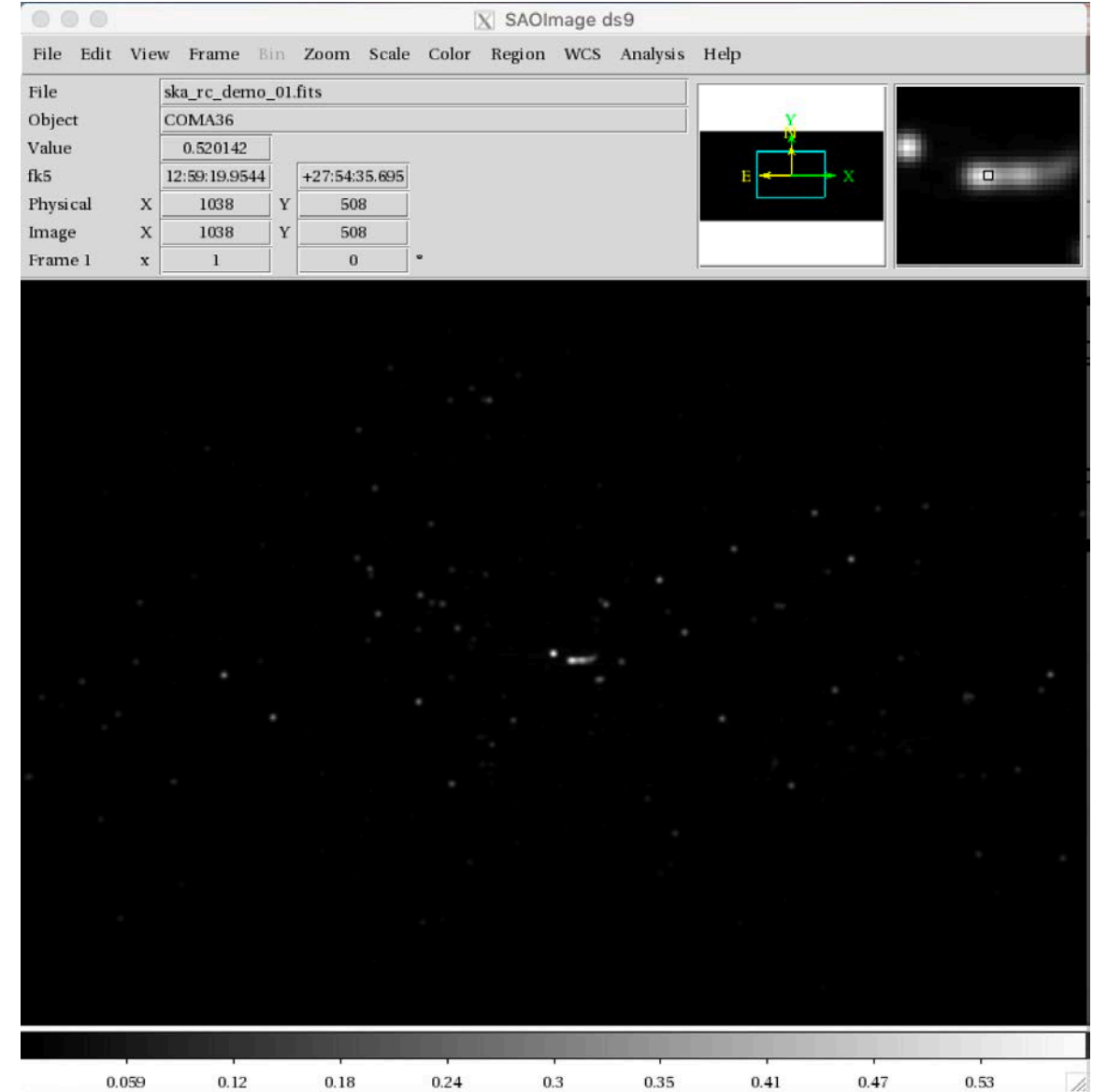




# The Prototype Step by Step (4.2.1)

```
bertocco — skarc001@ska01:~/data — ssh -XY skarc001@ska01.ira.inaf.it — 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)

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

`k3G5pg4Y6ETpHhP64BeK0VeCjgm7aBr5DWwucCpklTSPPMv4+2wqfYNhdxEVBuRglzl26q/83T/+WPfgX3cldR  
UO8hTYBOuBXQHfXuWbP1eYuQXR5o3fvueejhl4Y7XtfwV+5glfd3snzotXyZC+sZx0xrcHNHIGb2Nyb+SBPX2rh  
bkb/PvYbvhw9qLvbFdhf1ukirJmSSmEhT22HhgKLaa4BxUh6WwwTi1h6R7TXW40oBYs04Po/yLnzjHYfbEKMzU  
z6WcTkSicQwA/OkFCUoTzooiN/ franco.tinarelli@inaf.it`

Send

skarc.bo@ira.inaf.it 18:39 S

SKA RC IT: Access Information  
To: Franco Tinarelli

[Mail automatically generated, do not reply]  
Welcome to the SKA RC IT.  
We send you the link to retrieve your credentials  
for the use of data processing  
programs made available by the Regional Center.

with your public key.  
Username: skarc004

Best regards  
The SKA RC IT Staff

Send your ssh public keys  
to login without password



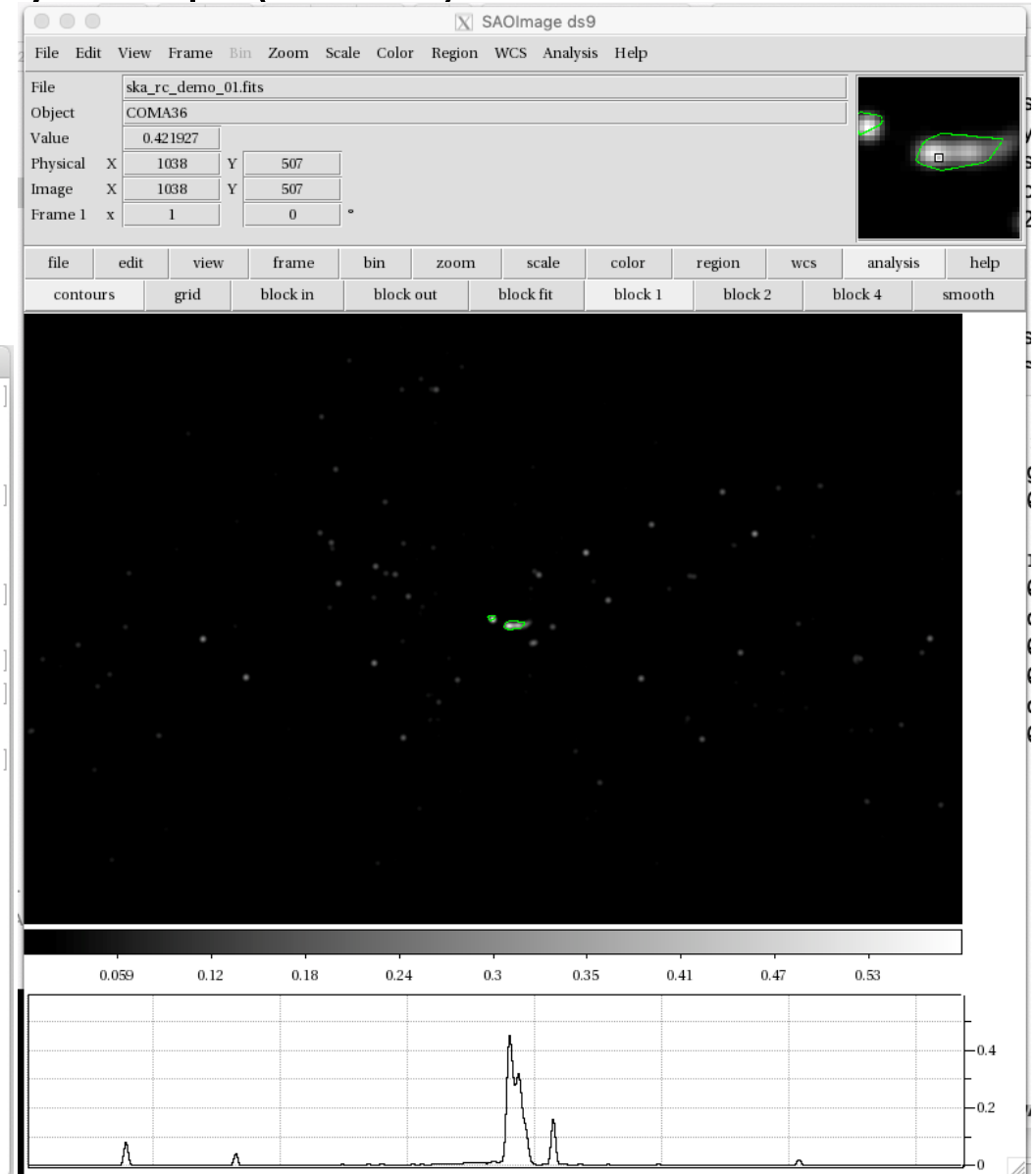


# The Prototype Step by Step (4.3.1)

Login without password and analyze data

```

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.Recurt



### 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.





# RAP and Grouper and the Account Linking

INTERNET®

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

<b>Added</b> attribute Unknown to a membership for member <a href="#">Franco Tinarelli (eduGAIN+Google+X.509)</a> .	2019/02/21 17:07 PM
<b>Added</b> <a href="#">Franco Tinarelli (eduGAIN+Google+X.509)</a> 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)

**Remote Authentication Portal**

**Guacamole**

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 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

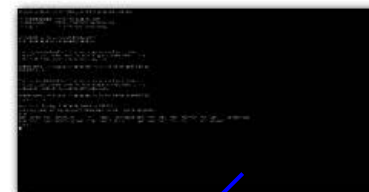
[Need help? Please read our User guide and FAQ.](#)

[Privacy policy](#)

localhost:8080/guacamole/#/?id\_token=eyJ0eXAiOiJKV1QiLCJhbG...

**RECENT CONNECTIONS**

sonia.zorba@inaf.it



test1

```
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
$
```

**ALL CONNECTIONS**

Filter

> test1

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



Thanks for your attention!

Questions?