Data exchange and computation between data centres using common A&A

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

INAF Science Archives & the Big Data Challenge – Roma, 17-19 June 2019

Use Case SKA Regional Centre (Aeneas WP6)

The AENEAS is a 3 year initiative funded by the Horizon 2020 program to develop a science-driven, functional design for a distributed, federated European Science Data Centre (ESDC) for the Square Kilometre Array.

WP6 will focus on processes, protocols, tools, and services required to ensure interoperability between existing SKA-relevant e-Infrastructures.

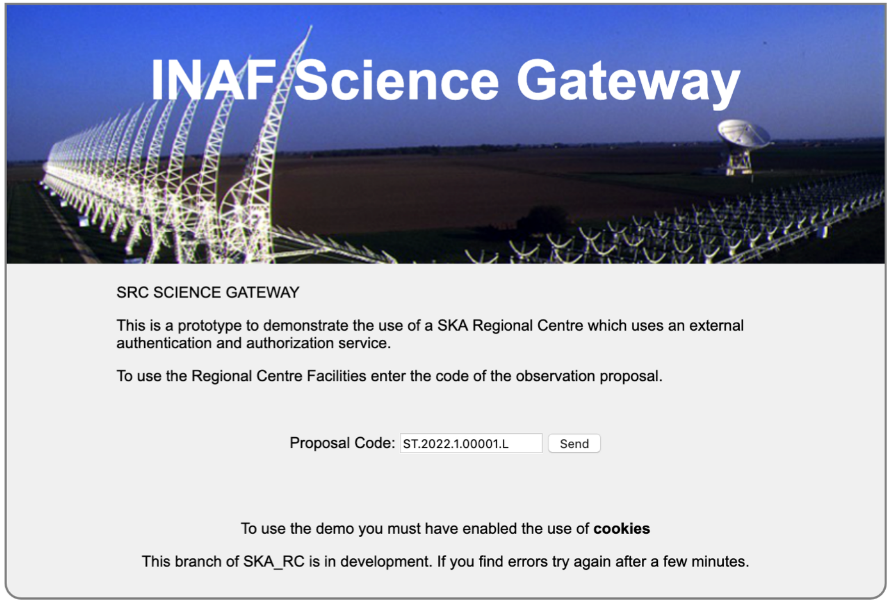
By addressing topics such as a seamless Authentication and Authorization Infrastructure (AAI) across the underlying network of service providers.

Essential to lower the barriers for potential users of the final SKA ESDC.

By enabling SKA users to access federated services and resources offered by different e-infrastructure providers in Europe and around the world.

WP6 is also crucial to connecting AENEAS with other similar efforts worldwide.

Prototype use case for SKA RC



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: ST.2022.1.00001.L Send

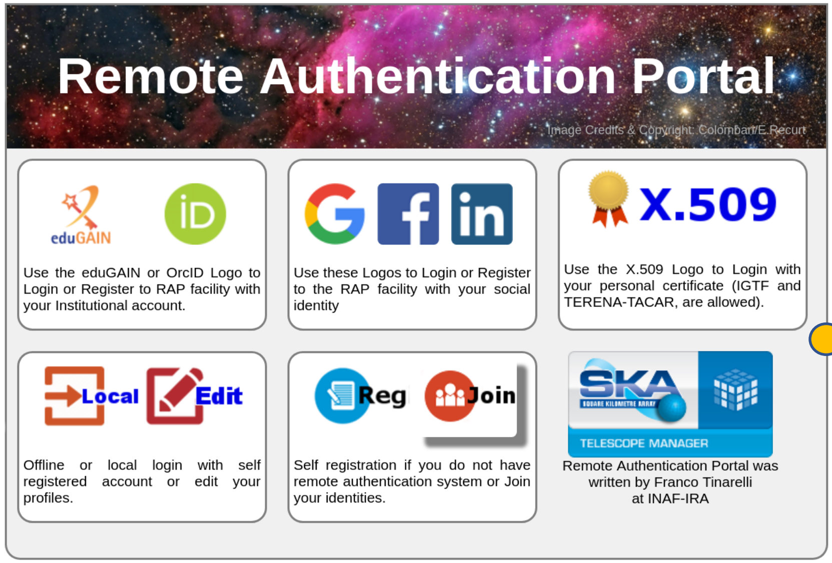
To use the demo you must have enabled the use of **cookies**

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

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

IN: Authentication

OUT: User Unique ID



Remote Authentication Portal
Image Credits & Copyright: Colombari/E.Recurt
eduGAIN
iD
X.509
Local
Edit
Reg
Join
SKA
SQUARE KILOMETRE ARRAY
TELESCOPE MANAGER

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).

Offline or local login with self registered account or edit your profiles.

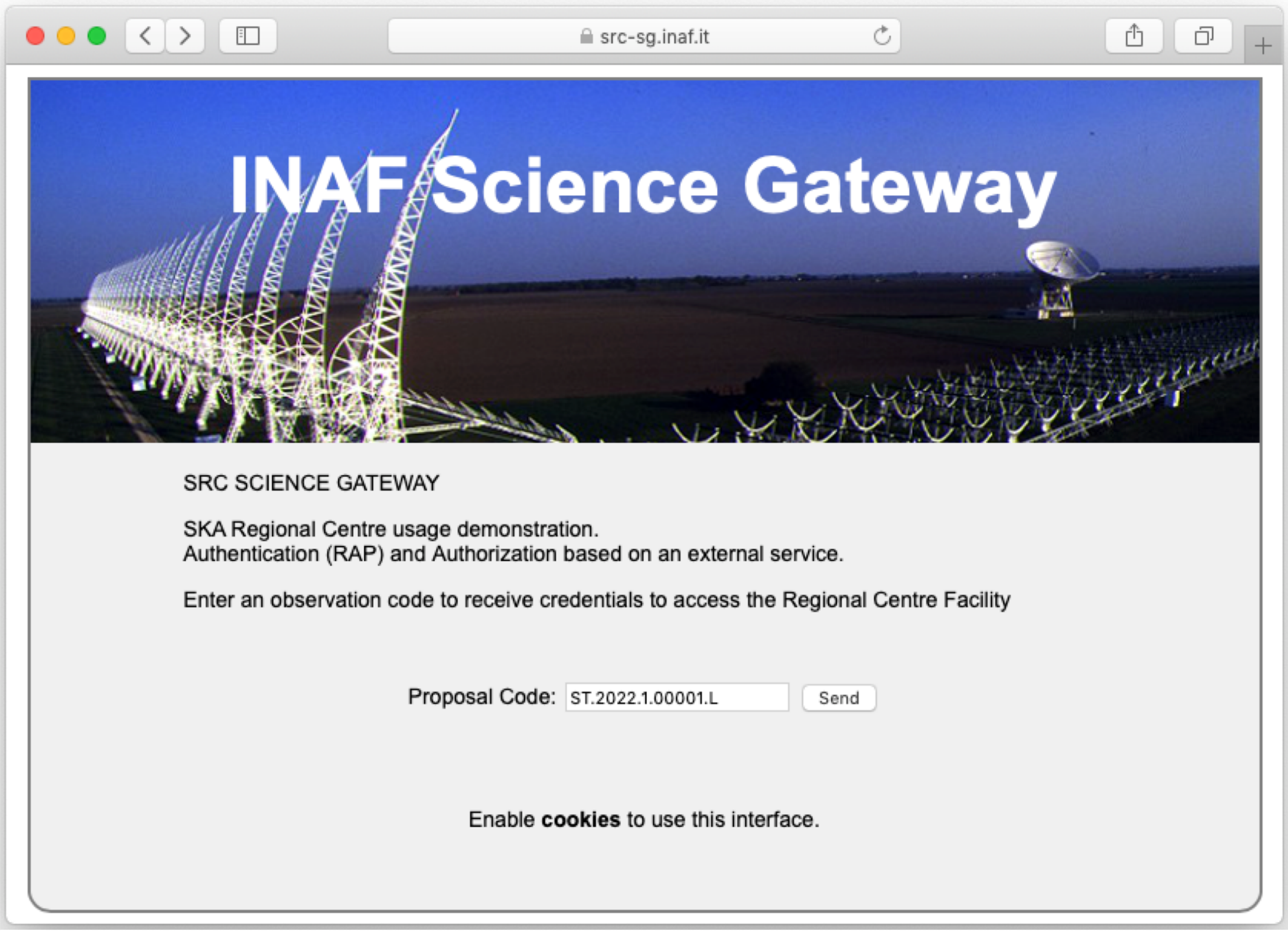
Self registration if you do not have remote authentication system or Join your identities.

Remote Authentication Portal was written by Franco Tinarelli at INAF-IRA

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

Grouper/GMS
IN: groupID, user_unique_ID
OUT: authorization

Actors: The Science Gateway



SRC SCIENCE GATEWAY

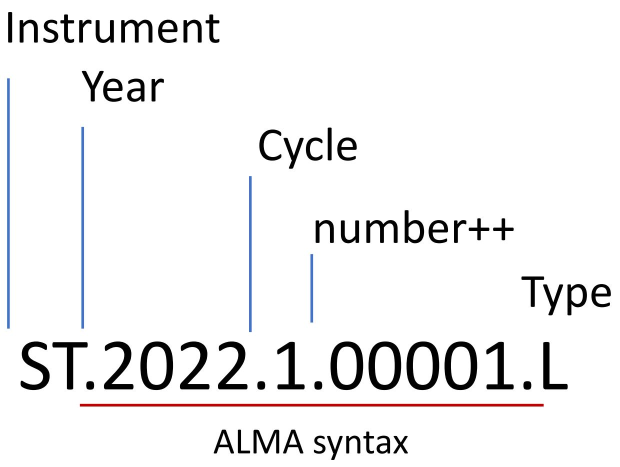
SKA Regional Centre usage demonstration.
Authentication (RAP) and Authorization based on an external service.

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

Proposal Code: ST.2022.1.00001.L Send

Enable **cookies** to use this interface.

- ➢ 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

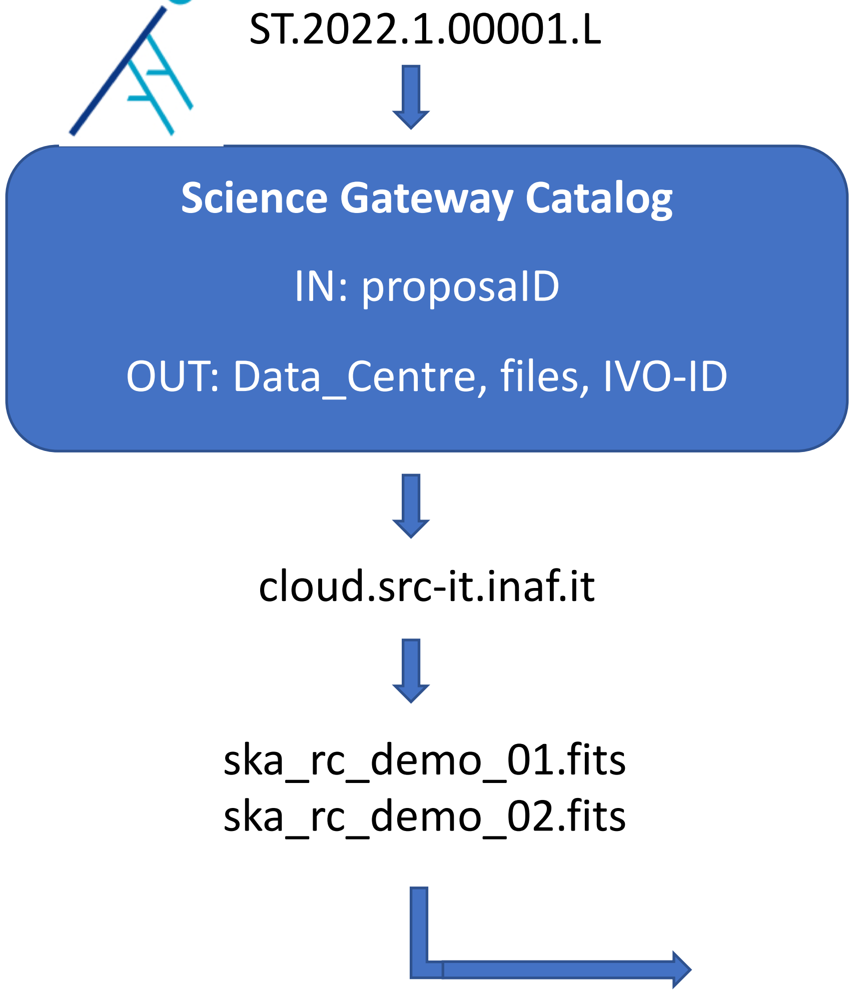
number++

Type

ST.2022.1.00001.L

ALMA syntax

Actors: The Science Gateway Catalog



ST.2022.1.00001.L

Science Gateway Catalog

IN: proposalD

OUT: Data_Centre, files, IVO-ID

cloud.src-it.inaf.it

ska_rc_demo_01.fits
ska_rc_demo_02.fits

The catalog contains information encoded using IVOA notation.

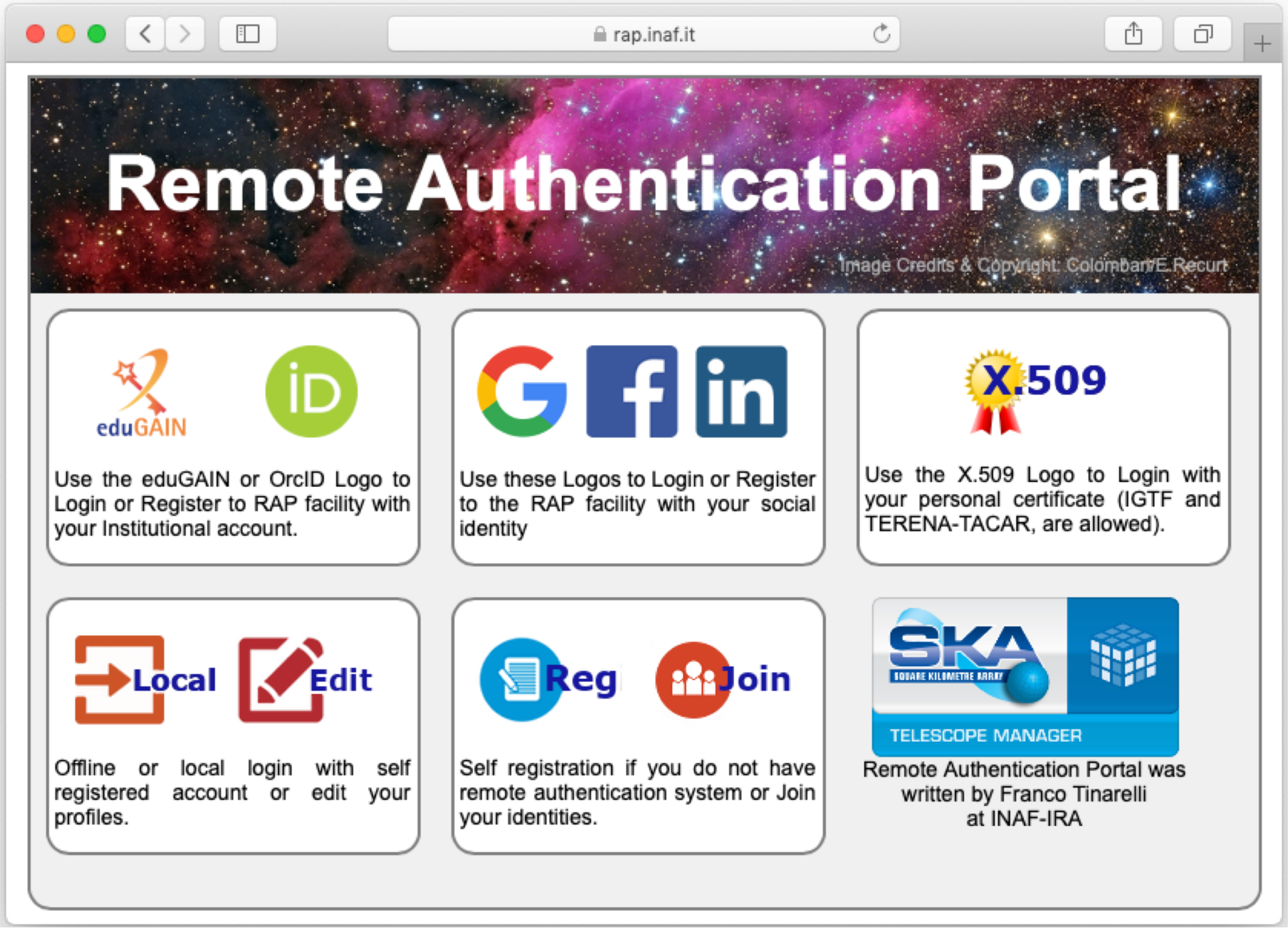
Group identifiers follow the GMS (current draft) specification, that embeds:

- 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 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).

Offline or local login with self registered account or edit your profiles.

Self registration if you do not have remote authentication system or Join your identities.

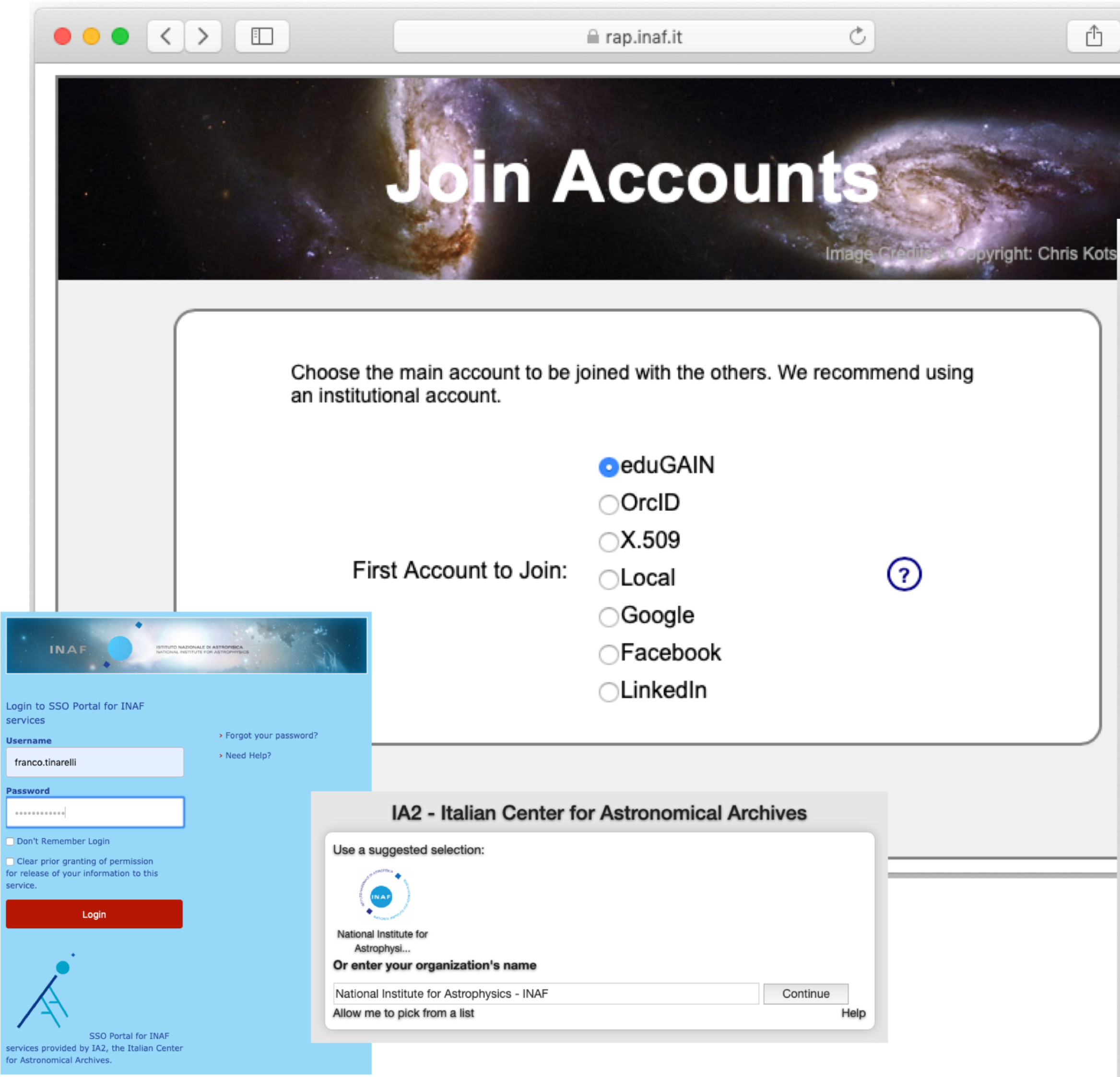
Remote Authentication Portal was written by Franco Tinarelli at INAF-IRA

(Use the link https://rap.inaf.it/Services/RAP 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.



rap.inaf.it

Join Accounts

Image Credit & Copyright: Chris Kots

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

First Account to Join:
● eduGAIN
○ OrcID
○ X.509
○ Local
○ Google
○ Facebook
○ LinkedIn

Login to SSO Portal for INAF services

Username: franco.tinarelli

Password: ••••••••••••

□ Don't Remember Login

□ Clear prior granting of permission for release of your information to this service.

Login

› Forgot your password?

› Need Help?

SSO Portal for INAF services provided by IA2, the Italian Center for Astronomical Archives.

IA2 - Italian Center for Astronomical Archives

Use a suggested selection:

National Institute for Astrophysi...

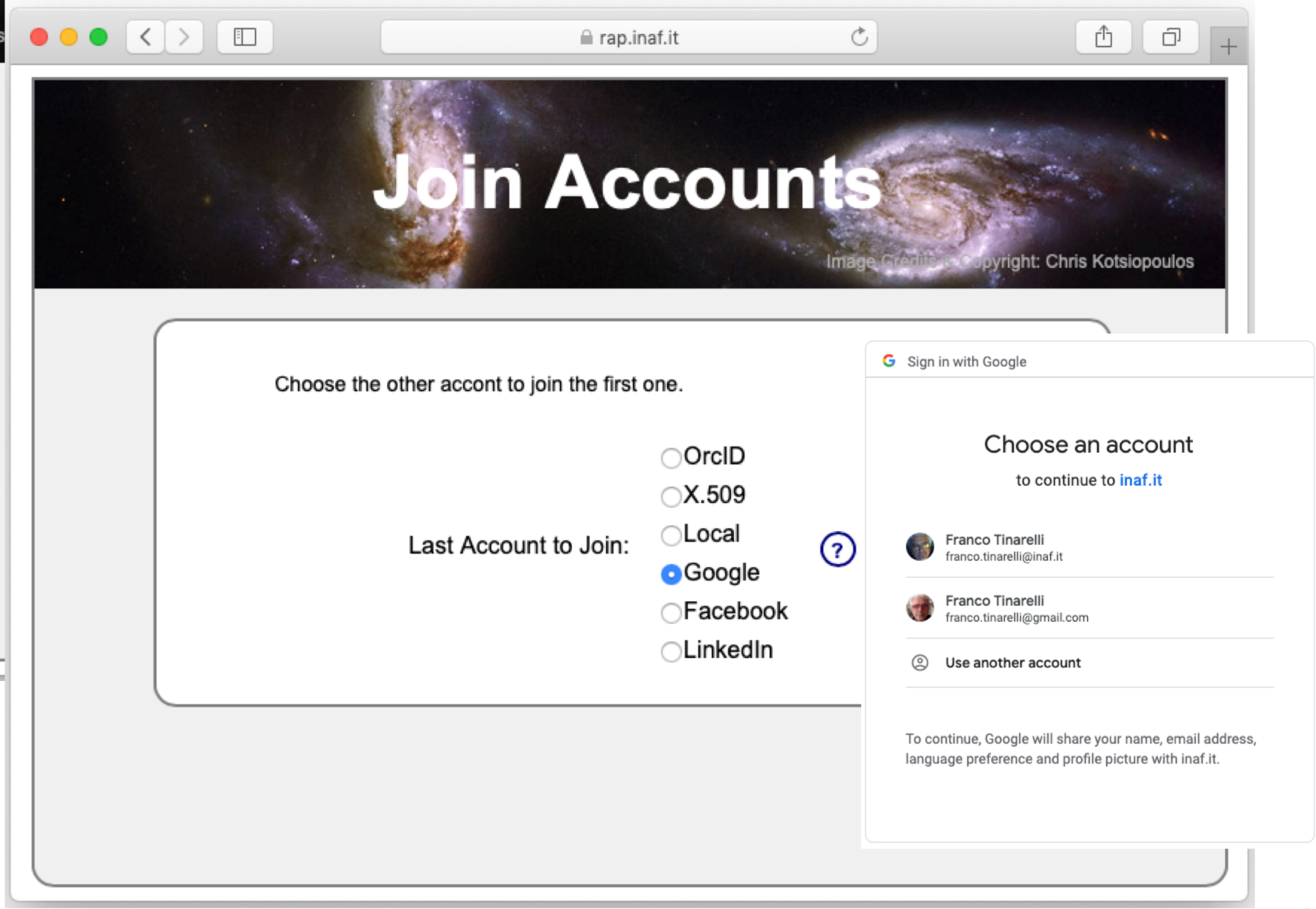
Or enter your organization's name

National Institute for Astrophysics - INAF

Continue

Allow me to pick from a list

Help



rap.inaf.it

Join Accounts

Image Credit & Copyright: Chris Kotsiopoulos

Choose the other accont to join the first one.

Last Account to Join:
○ OrcID
○ X.509
○ Local
● Google
○ Facebook
○ LinkedIn

Sign in with Google

Choose an account

to continue to inaf.it

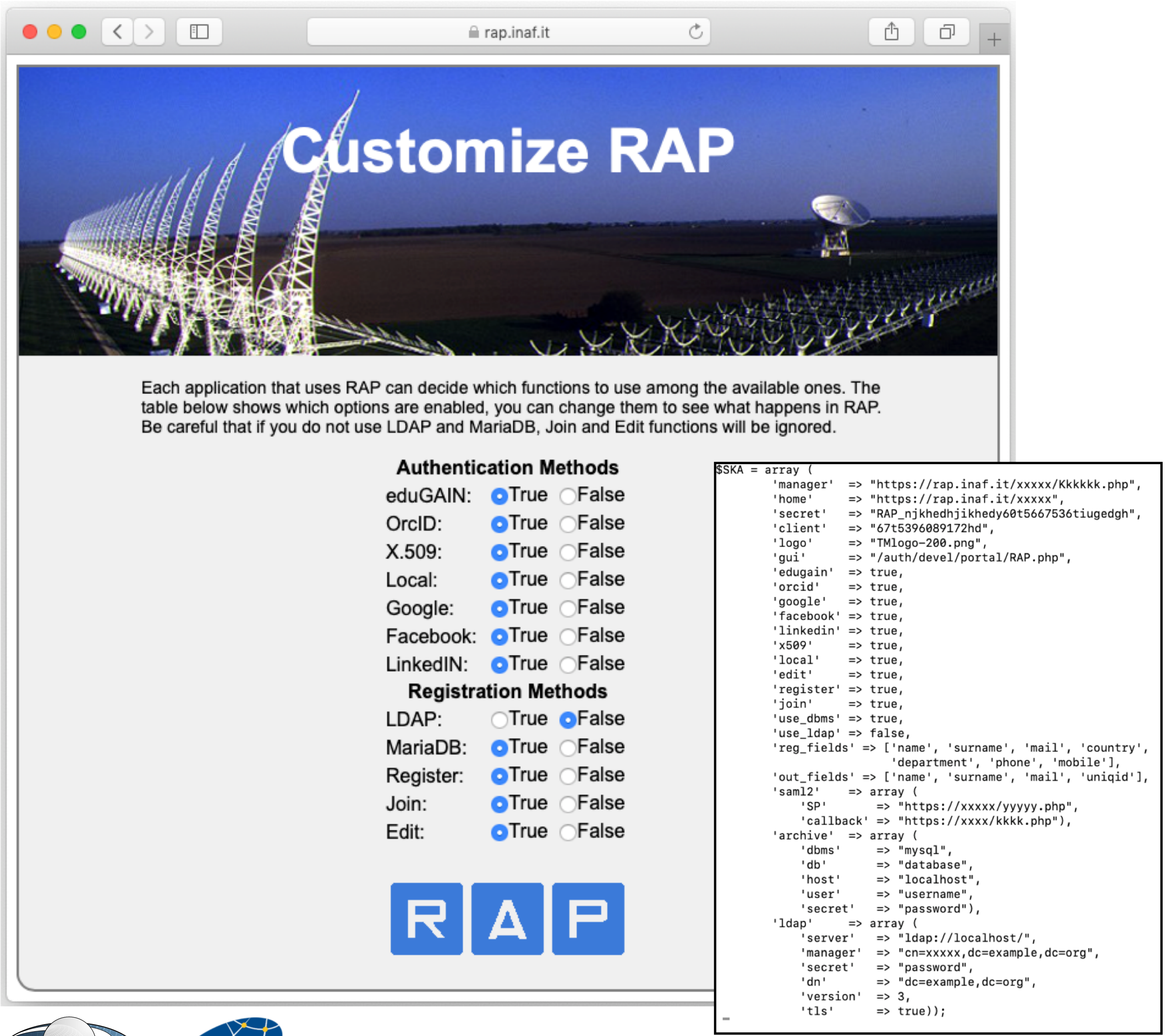
Franco Tinarelli
franco.tinarelli@inaf.it

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.

Actors: RAP and the 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

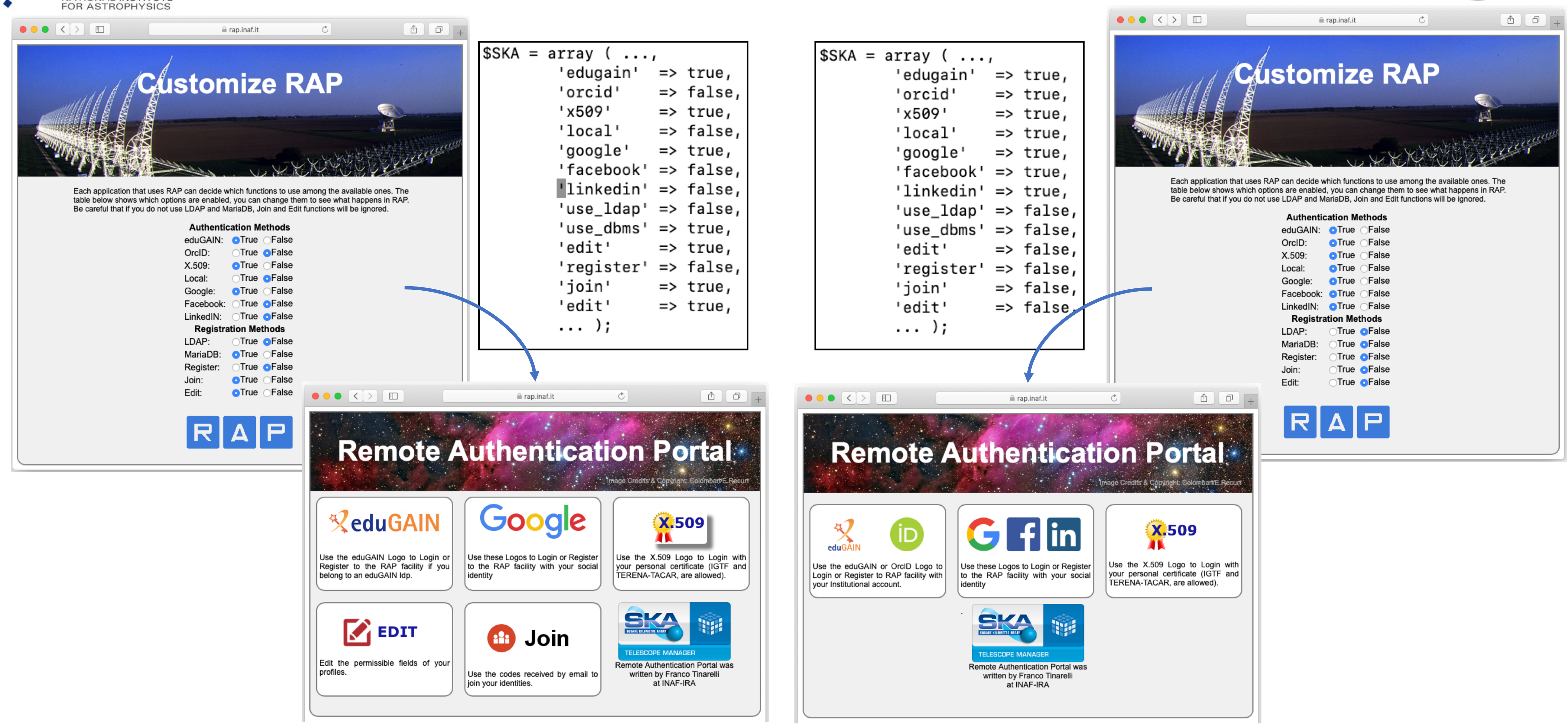
```
$SKA = array (
        'manager'  => "https://rap.inaf.it/xxxxx/Kkkkkk.php",
        'home'     => "https://rap.inaf.it/xxxxx",
        'secret'   => "RAP_njkhedhjikhedy60t5667536tiugedgh",
        'client'   => "67t5396089172hd",
        'logo'     => "TMlogo-200.png",
        'gui'      => "/auth/devel/portal/RAP.php",
        '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 Customized Layouts



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

```
$SKA = array ( ...,
          'edugain'  => true,
          'orcid'    => false,
          'x509'     => true,
          'local'    => false,
          'google'   => true,
          'facebook' => false,
          'linkedin' => false,
          'use_ldap' => false,
          'use_dbms' => true,
          'edit'     => true,
          'register' => false,
          'join'     => true,
          'edit'     => true,
          ... );
```

```
$SKA = array ( ...,
          'edugain'  => true,
          'orcid'    => true,
          'x509'     => true,
          'local'    => true,
          'google'   => true,
          'facebook' => true,
          'linkedin' => true,
          'use_ldap' => false,
          'use_dbms' => false,
          'edit'     => false,
          'register' => false,
          'join'     => false,
          'edit'     => false,
          ... );
```

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

Remote Authentication Portal

Image Credits & Copyright: Colombari/E.Recurt

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).

Edit the permissible fields of your profiles.

Use the codes received by email to join your identities.

Remote Authentication Portal was written by Franco Tinarelli at INAF-IRA

Remote Authentication Portal

Image Credits & Copyright: Colombari/E.Recurt

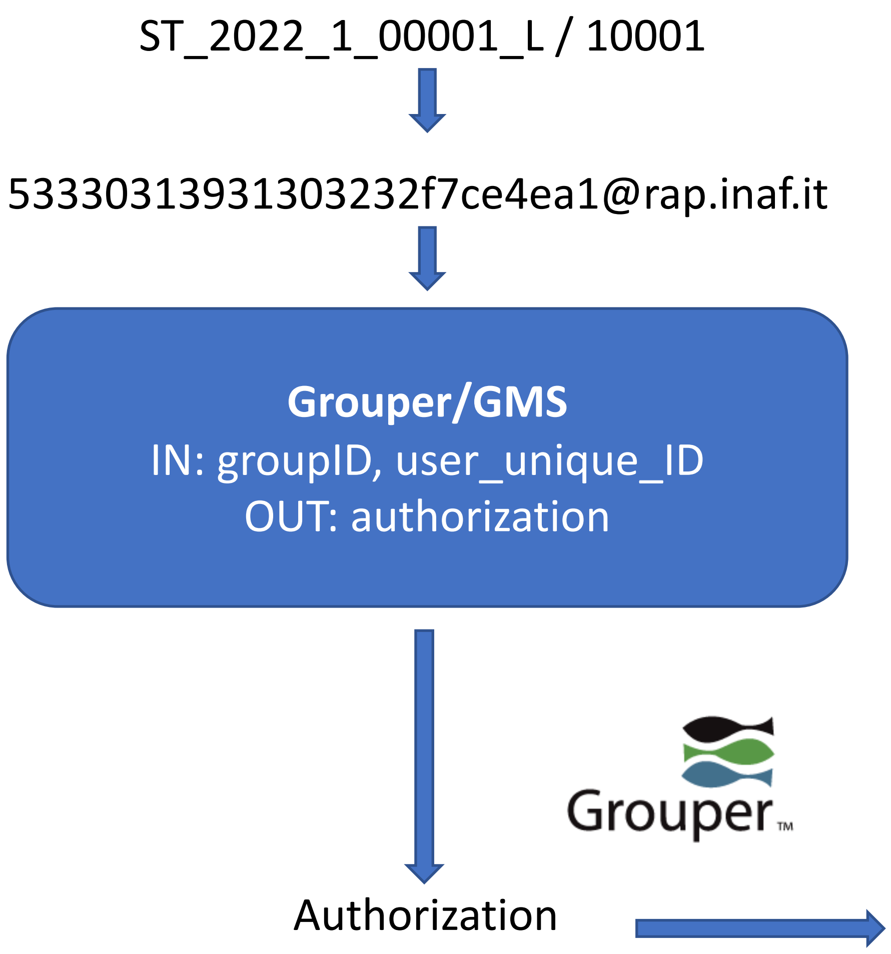
Use the eduGAIN or OrcID Logo to Login or Register to RAP facility with your Institutional account.

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

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

Remote Authentication Portal was written by Franco Tinarelli at INAF-IRA

Actors: The Science Gateway GMS



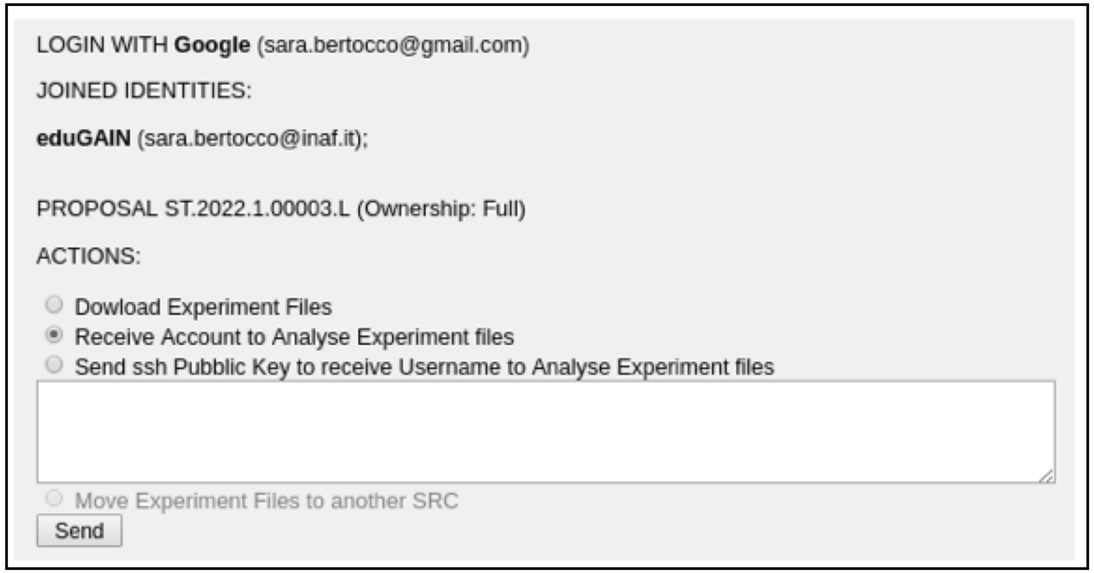
ST_2022_1_00001_L / 10001

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);

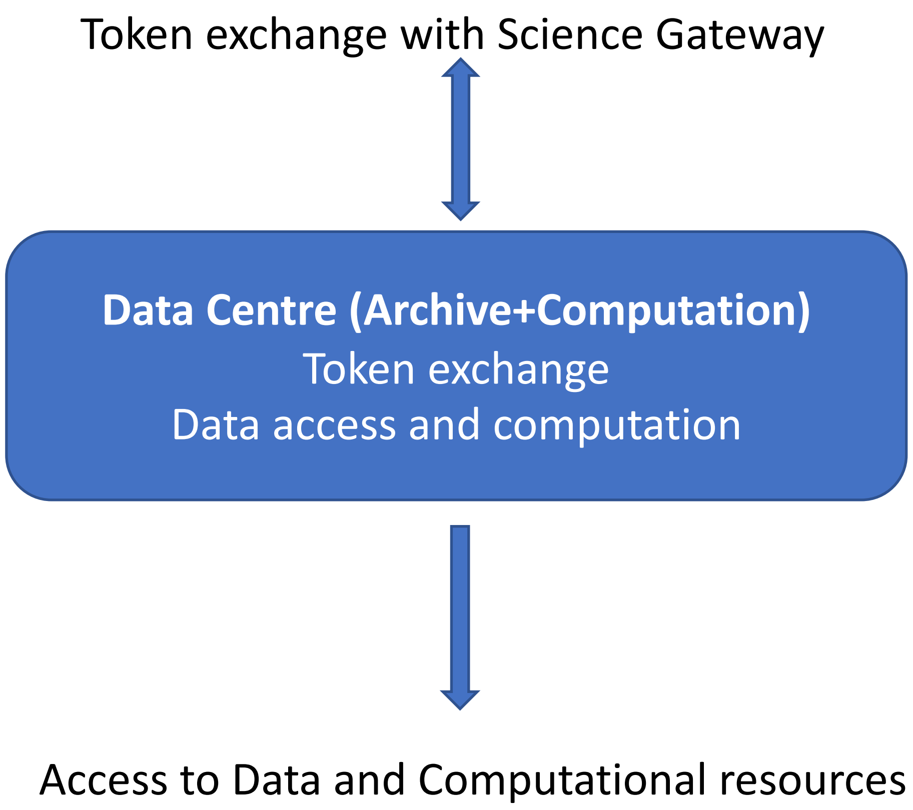
PROPOSAL ST.2022.1.00003.L (Ownership: Full)

ACTIONS:

○ Dowload Experiment Files
● Receive Account to Analyse Experiment files
○ Send ssh Pubblic Key to receive Username to Analyse Experiment files

○ Move Experiment Files to another SRC

Actors: The Data Centre

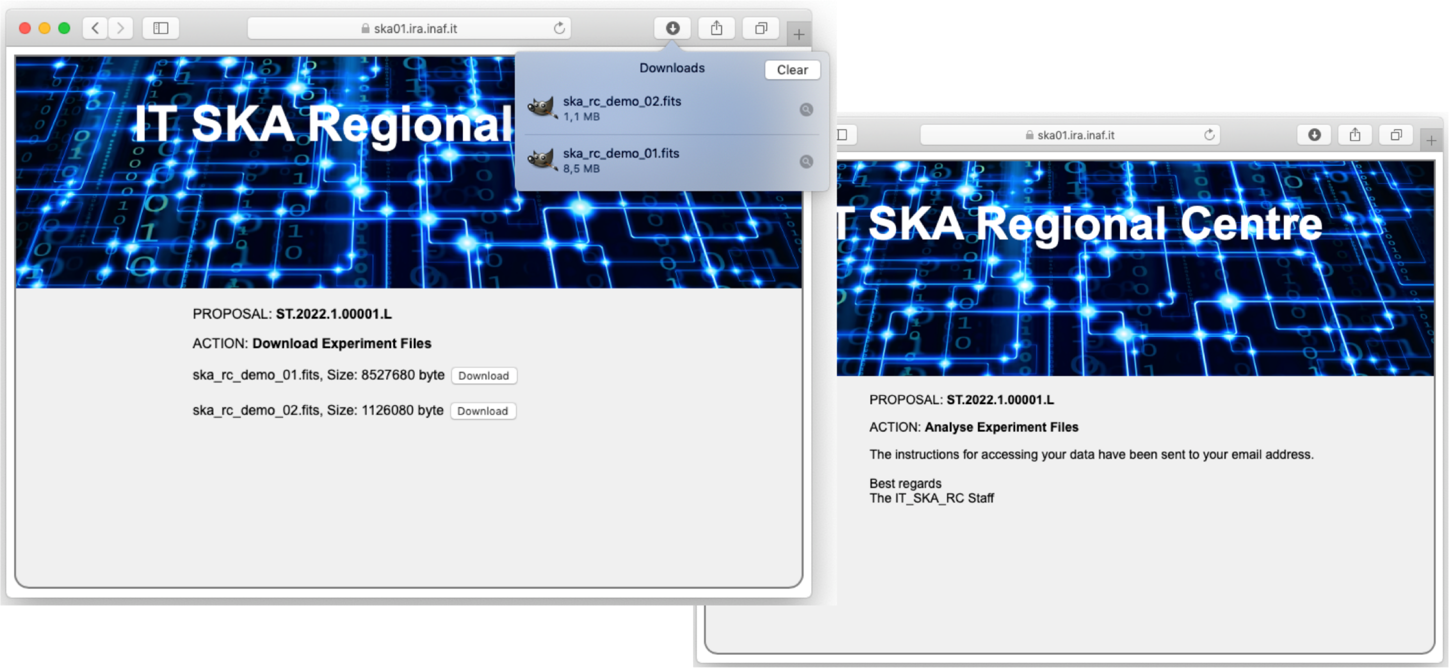


Token exchange with Science Gateway

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.



PROPOSAL: **ST.2022.1.00001.L**

ACTION: **Download Experiment Files**

ska_rc_demo_01.fits, Size: 8527680 byte Download

ska_rc_demo_02.fits, Size: 1126080 byte Download

PROPOSAL: **ST.2022.1.00001.L**

ACTION: **Analyse Experiment Files**

The instructions for accessing your data have been sent to your email address.

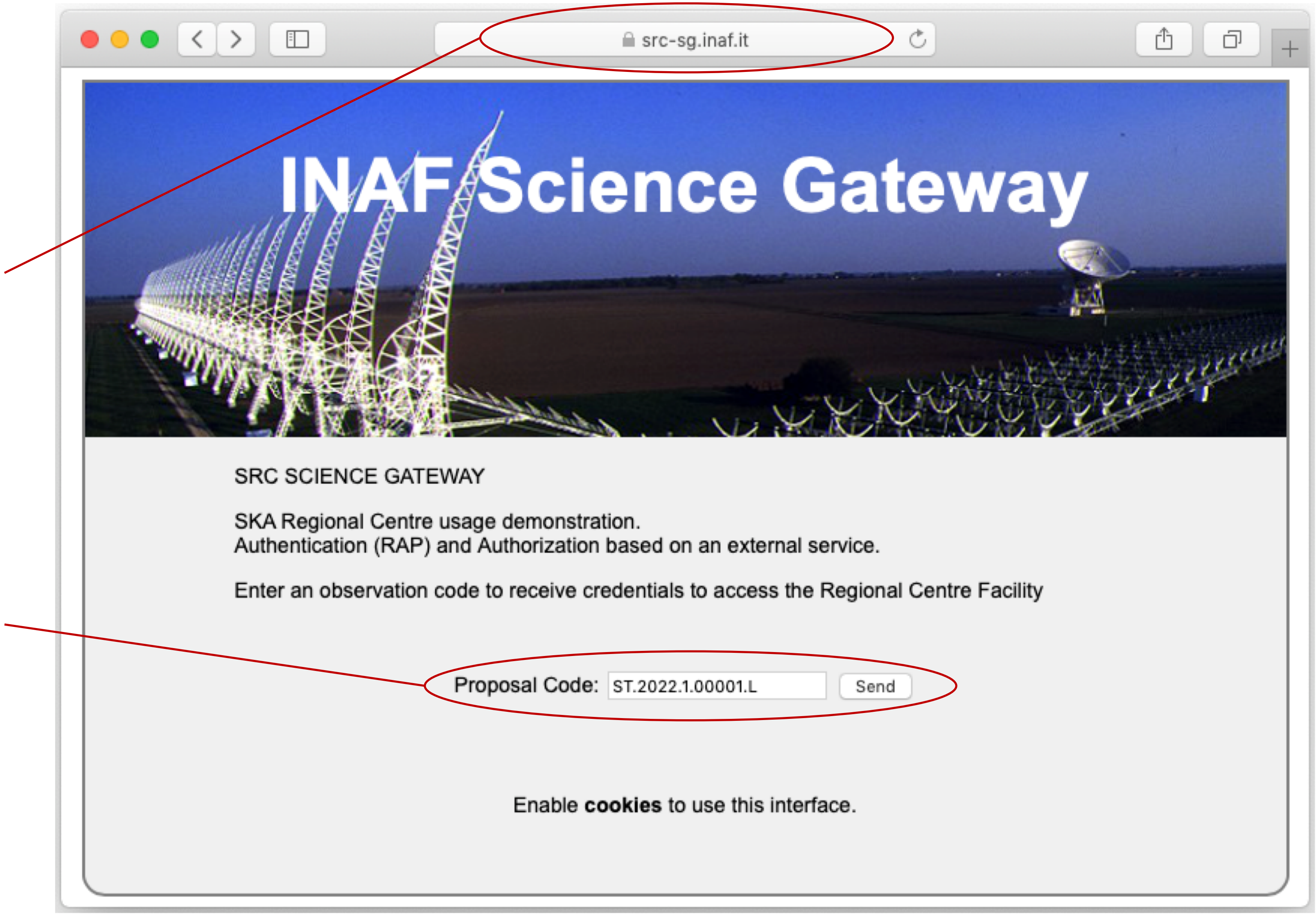
Best regards
The IT_SKA_RC Staff

The Prototype Step by Step (1)

Call Science Gateway

And

Insert the Proposal ID



SRC SCIENCE GATEWAY

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

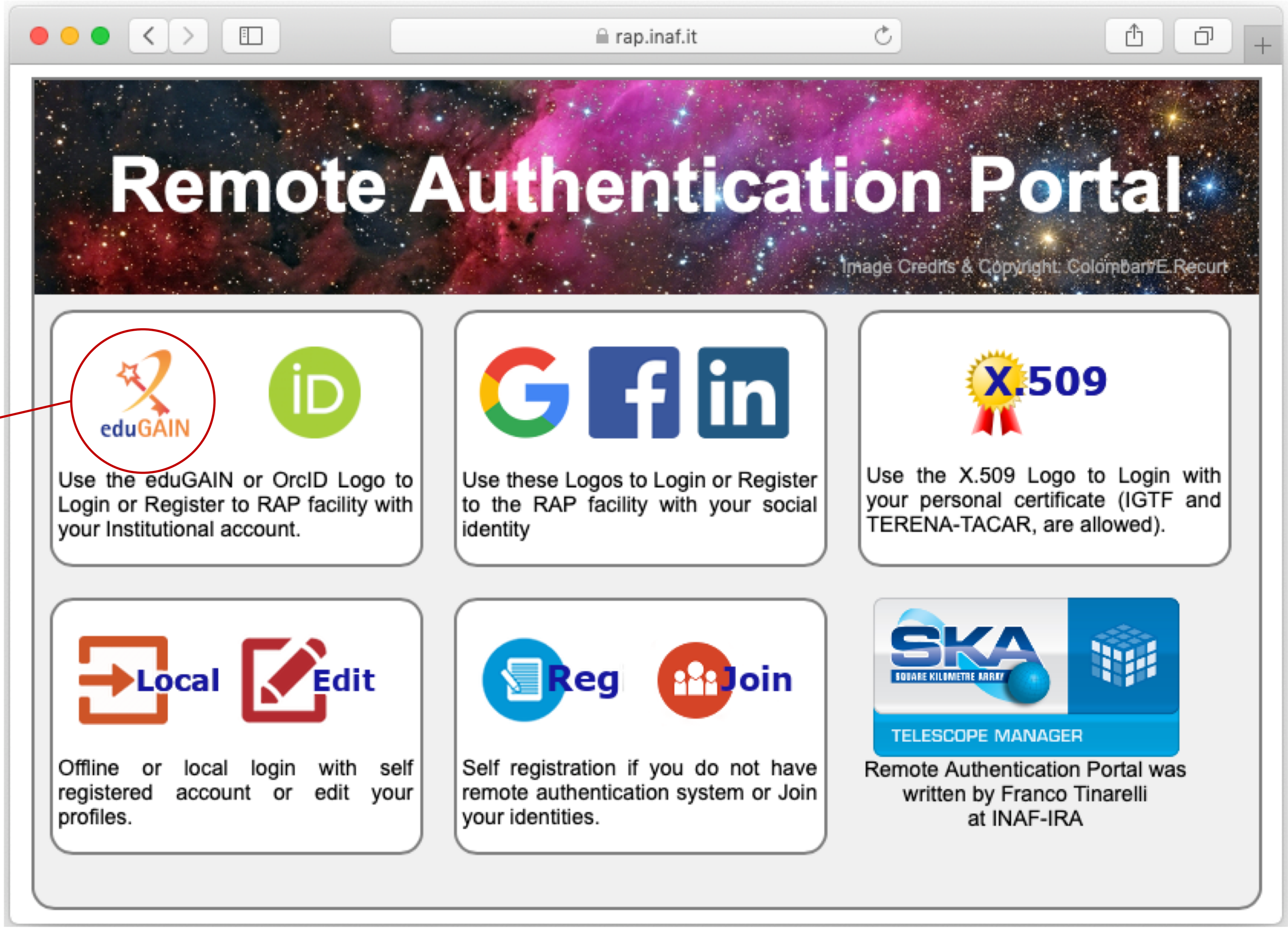
Enter an observation code to receive credentials to access the Regional Centre Facility

Proposal Code: ST.2022.1.00001.L Send

Enable **cookies** to use this interface.

The Prototype Step by Step (2)

Authenticate Yourself



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

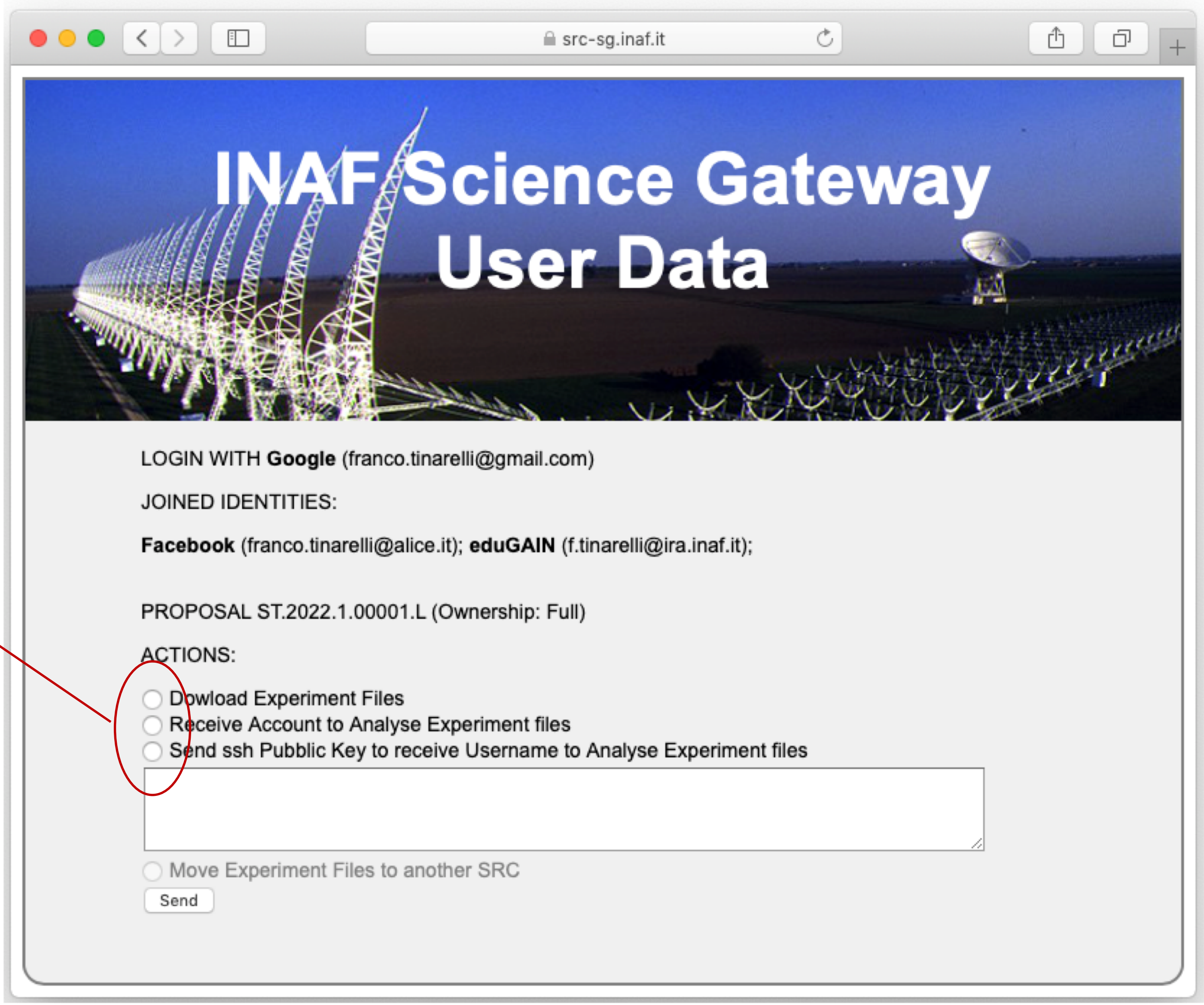
Offline or local login with self registered account or edit your profiles.

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

The Prototype Step by Step (3)

Select the actions to manage your 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)

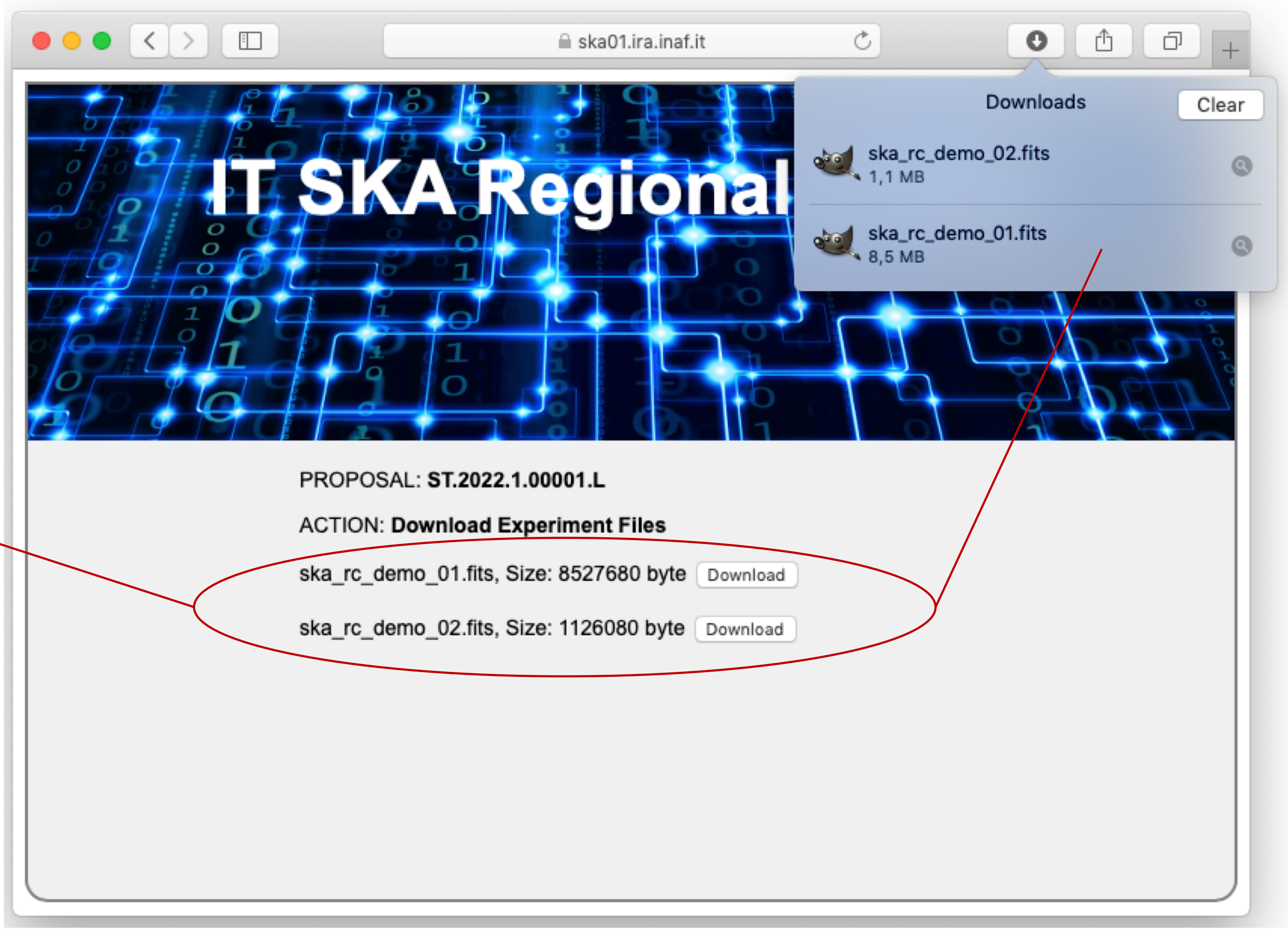
ACTIONS:

○ Dowload Experiment Files
○ Receive Account to Analyse Experiment files
○ Send ssh Pubblic Key to receive Username to Analyse Experiment files

○ Move Experiment Files to another SRC

The Prototype Step by Step (4.1)

Dowload experiment files



PROPOSAL: **ST.2022.1.00001.L**

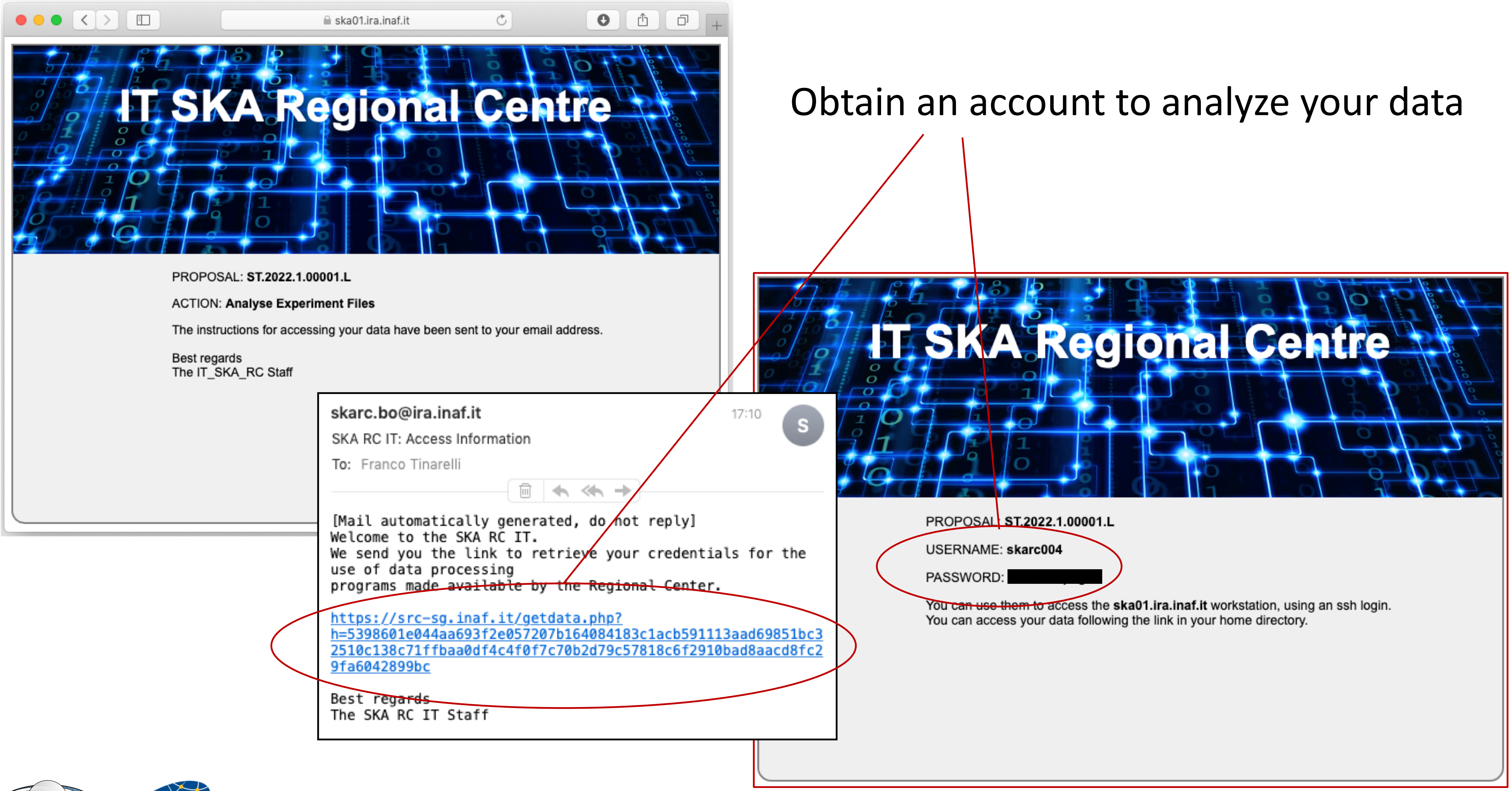
ACTION: **Download Experiment Files**

ska_rc_demo_01.fits, Size: 8527680 byte Download

ska_rc_demo_02.fits, Size: 1126080 byte Download

The Prototype Step by Step (4.2)

Obtain an account to analyze your data



PROPOSAL: **ST.2022.1.00001.L**

ACTION: **Analyse Experiment Files**

The instructions for accessing your data have been sent to your email address.

Best regards
The IT_SKA_RC Staff

skarc.bo@ira.inaf.it 17:10

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.

https://src-sg.inaf.it/getdata.php?
h=5398601e044aa693f2e057207b164084183c1acb591113aad69851bc3
2510c138c71ffbaa0df4c4f0f7c70b2d79c57818c6f2910bad8aacd8fc2
9fa6042899bc

Best regards
The SKA RC IT Staff
```

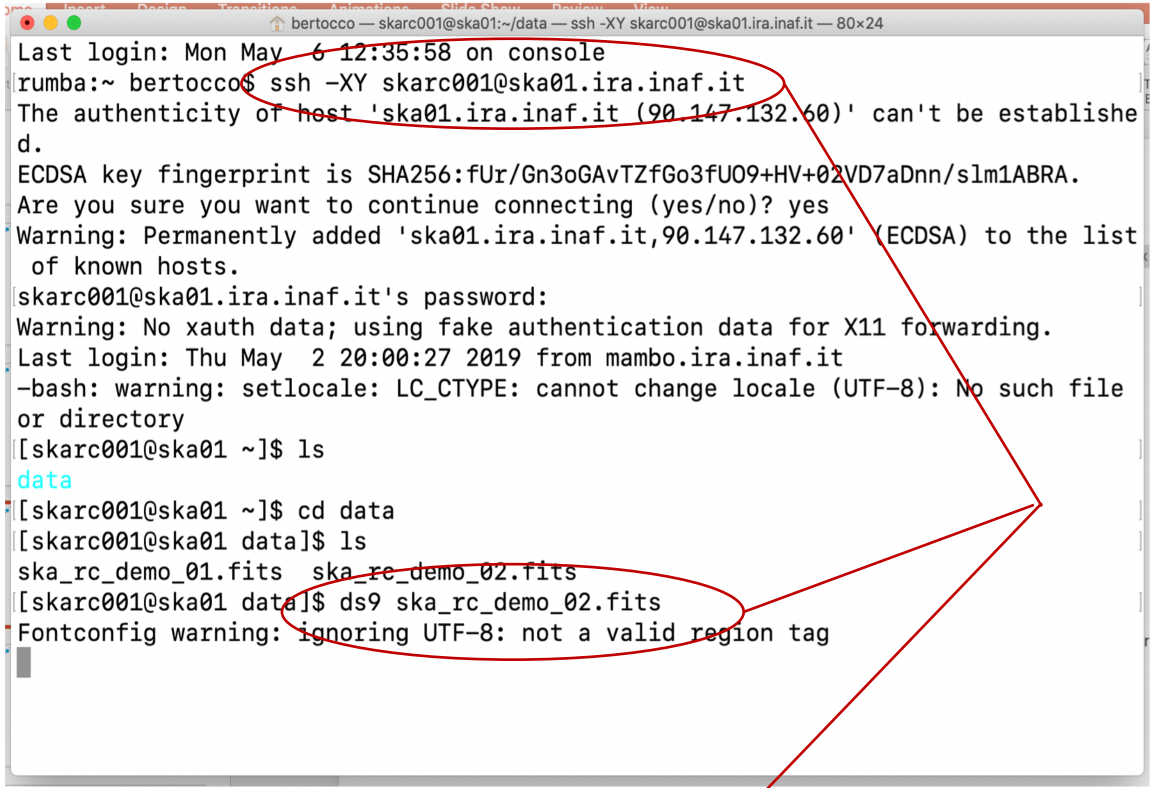
PROPOSAL: **ST.2022.1.00001.L**

USERNAME: **skarc004**

PASSWORD: [redacted]

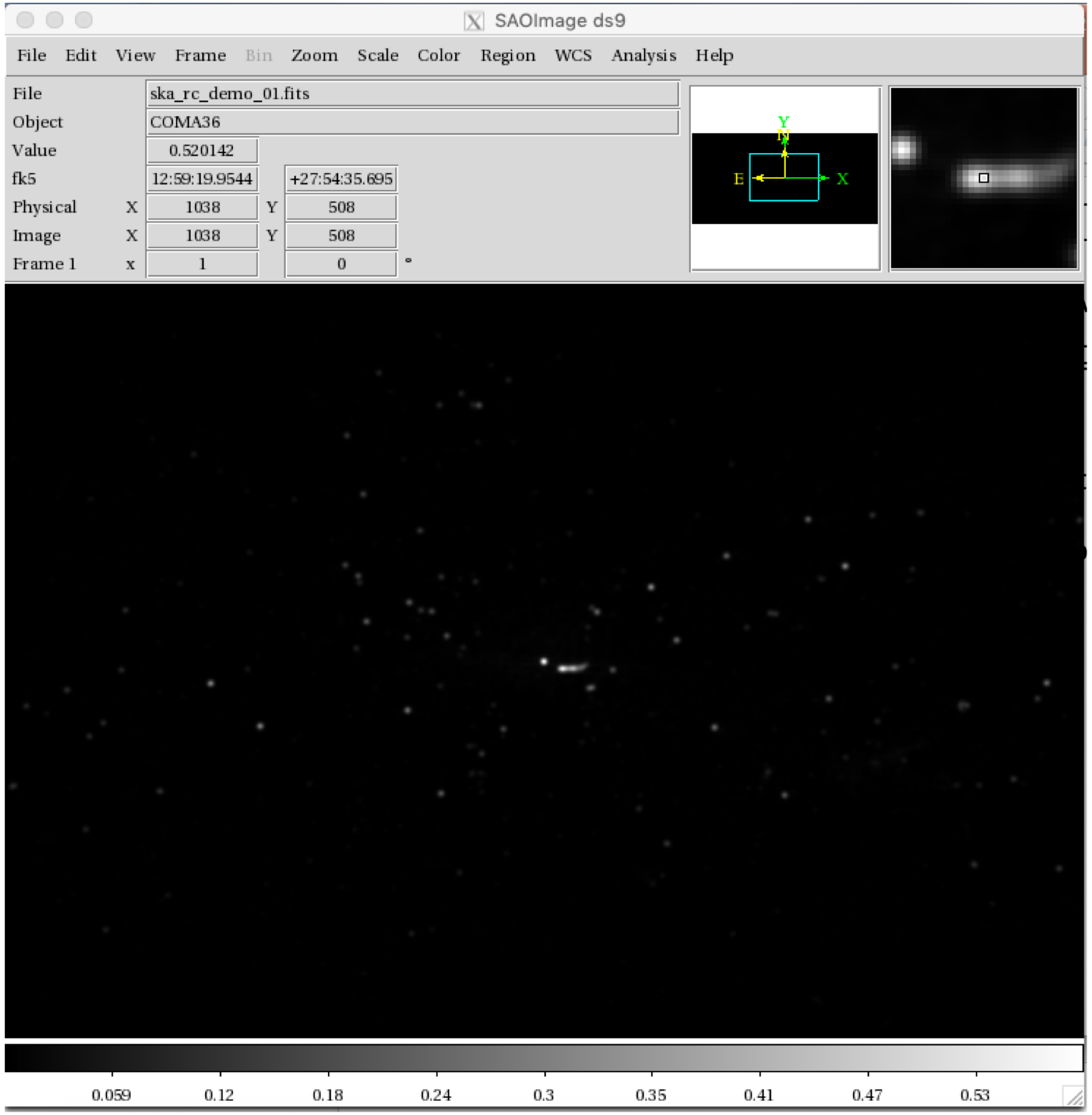
You can use them to access the **ska01.ira.inaf.it** workstation, using an ssh login.
You can access your data following the link in your home directory.

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
```

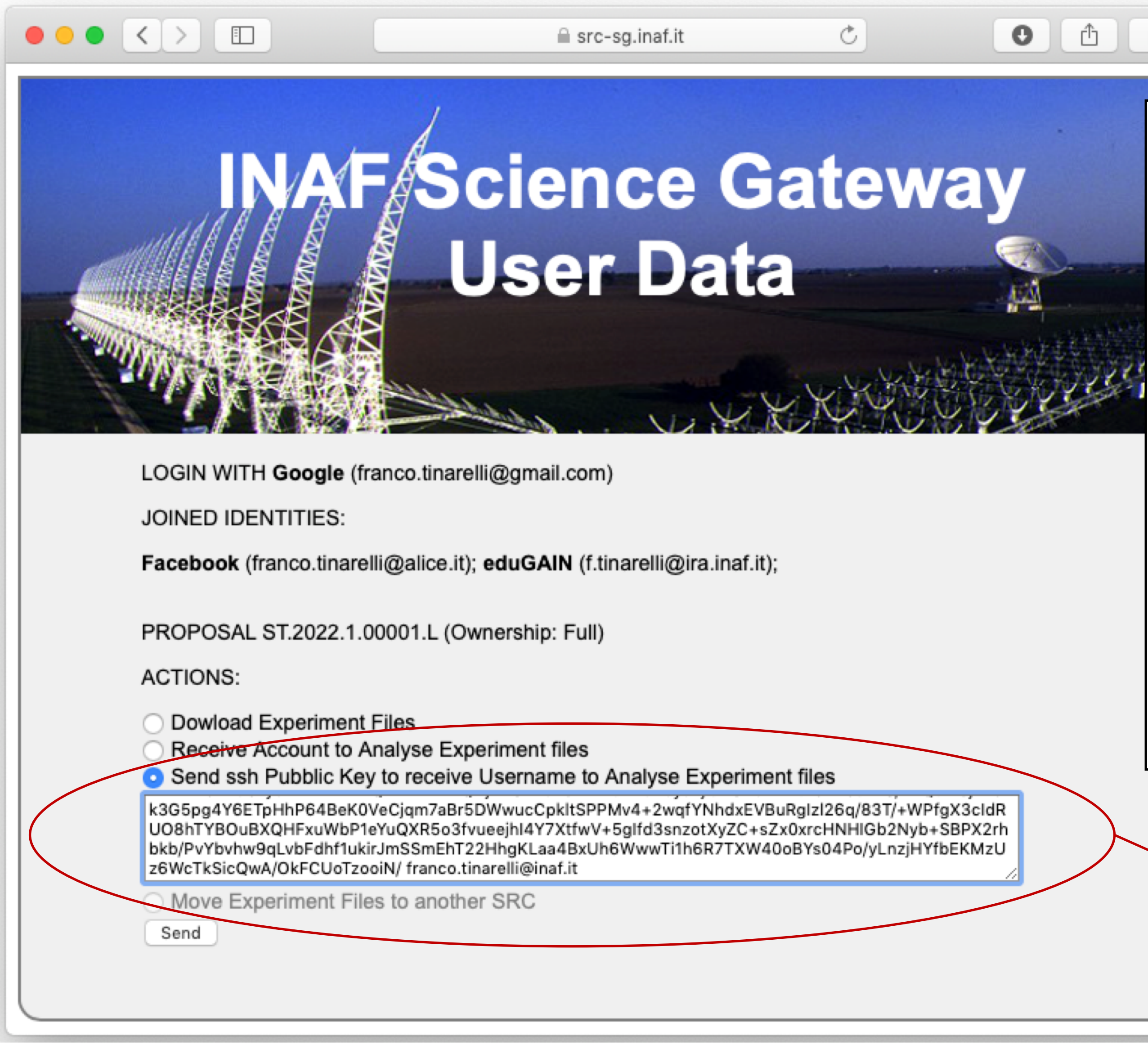


SAOImage ds9

File: ska_rc_demo_01.fits
Object: COMA36
Value: 0.520142
fk5: 12:59:19.9544 +27:54:35.695
Physical X 1038 Y 508
Image X 1038 Y 508
Frame 1 x 1 0 °

Login to computing element
and analyze data

The Prototype Step by Step (4.3)



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)

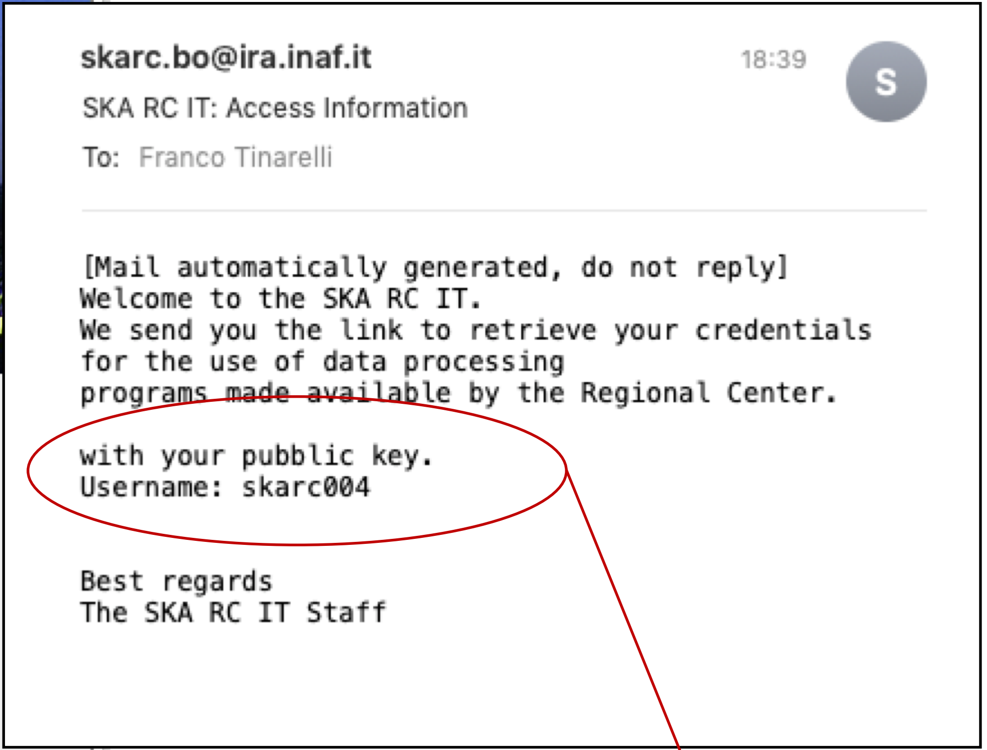
ACTIONS:

○ Dowload Experiment Files
○ Receive Account to Analyse Experiment files
● Send ssh Pubblic Key to receive Username to Analyse Experiment files

```
k3G5pg4Y6ETpHhP64BeK0VeCjqm7aBr5DWwucCpkltSPPMv4+2wqfYNhdxEVBuRglzl26q/83T/+WPfgX3cldR
UO8hTYBOuBXQHFxuWbP1eYuQXR5o3fvueejhl4Y7XtfwV+5glfd3snzotXyZC+sZx0xrcHNHIGb2Nyb+SBPX2rh
bkb/PvYbvhw9qLvbFdhf1ukirJmSSmEhT22HhgKLaa4BxUh6WwwTi1h6R7TXW40oBYs04Po/yLnzjHYfbEKMzU
z6WcTkSicQwA/OkFCUoTzooiN/ franco.tinarelli@inaf.it
```

○ Move Experiment Files to another SRC

Send



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

SKA RC IT: Access Information

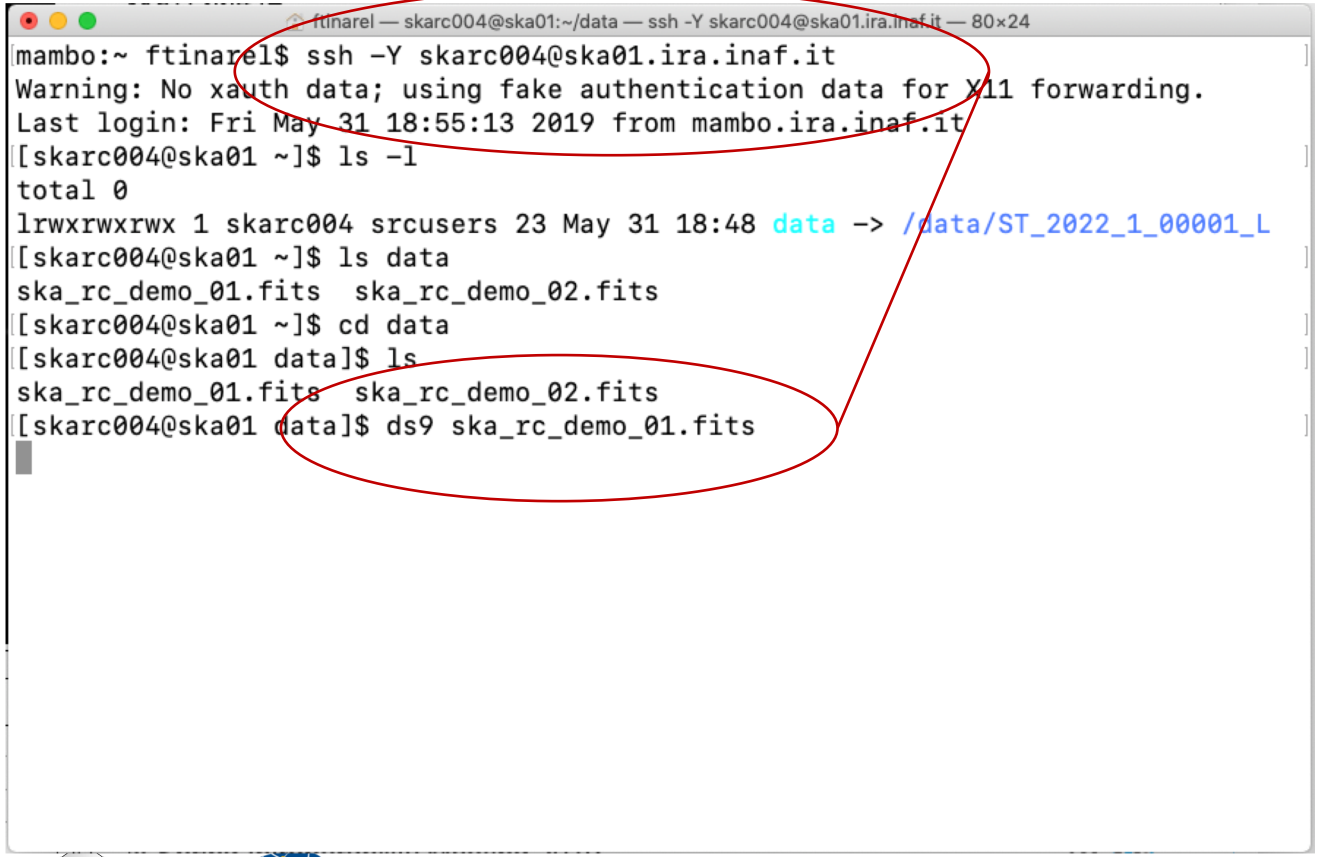
To: Franco Tinarelli

```
[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 pubblic key.
Username: skarc004

Best regards
The SKA RC IT Staff
```

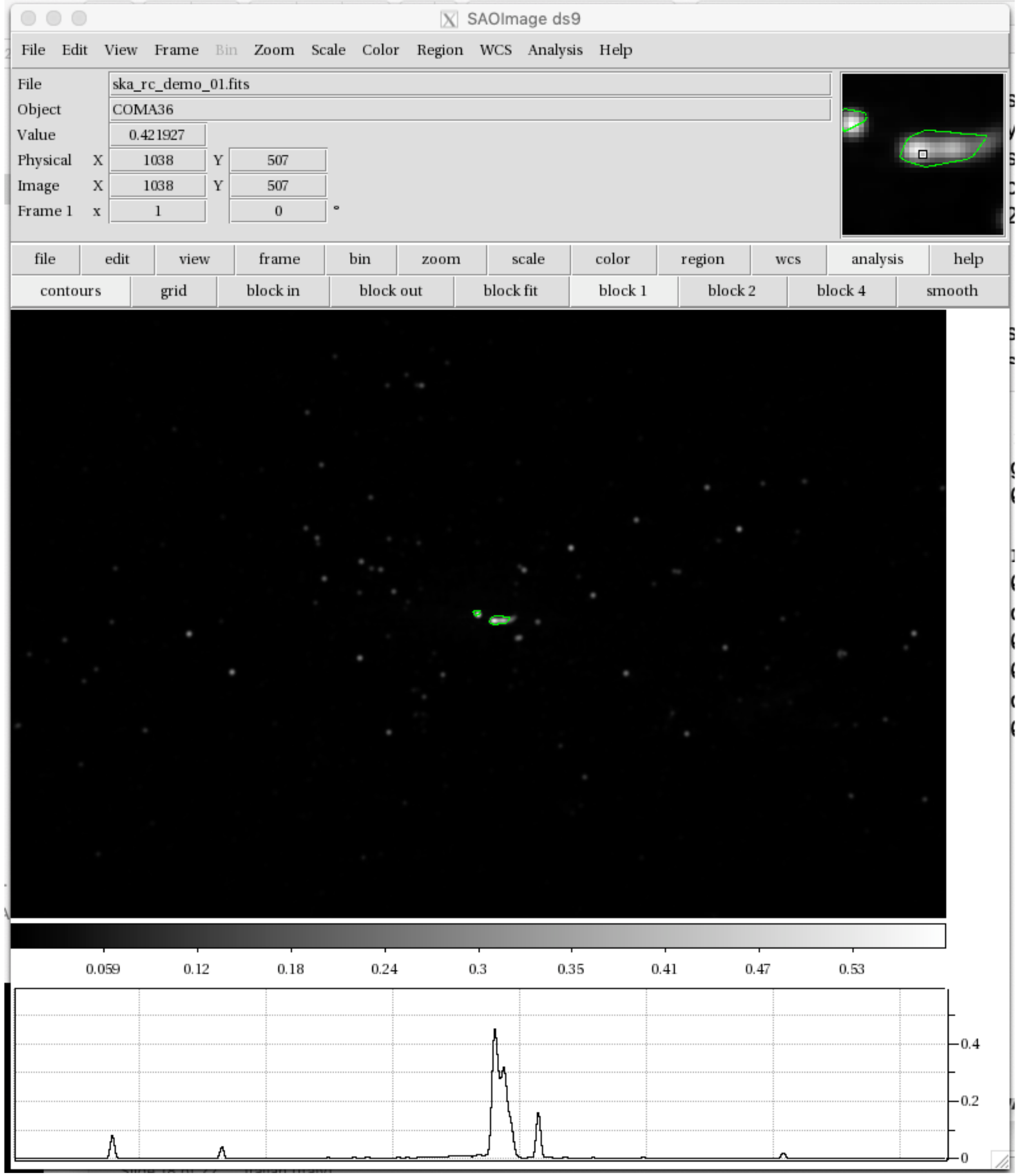
Send your ssh public keys to login without password

The Prototype Step by Step (4.3.1)

Login without password and analyze data


ftinarel — skarc004@ska01:~/data — ssh -Y skarc004@ska01.ira.inaf.it — 80×24

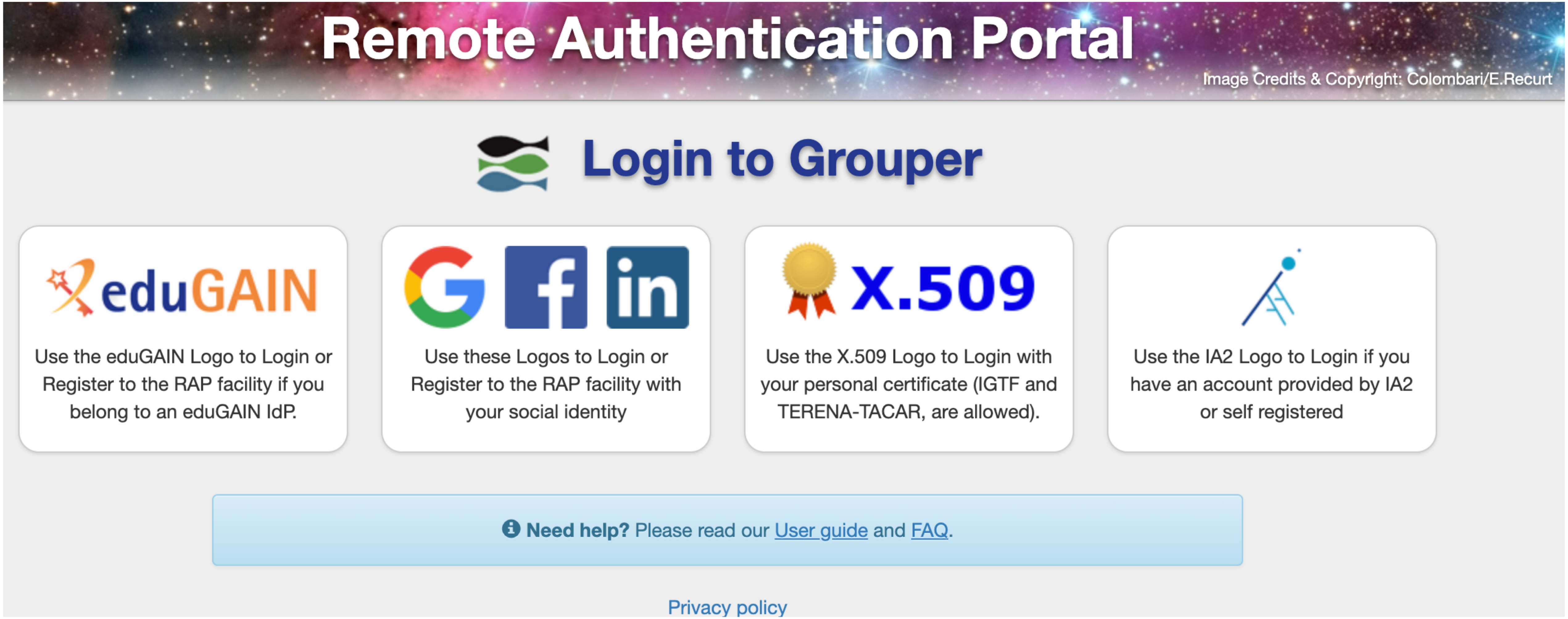
```
mambo:~ ftinarel$ ssh -Y skarc004@ska01.ira.inaf.it
Warning: No xauth data; using fake authentication data for X11 forwarding.
Last login: Fri May 31 18:55:13 2019 from mambo.ira.inaf.it
[skarc004@ska01 ~]$ ls -l
total 0
lrwxrwxrwx 1 skarc004 srcusers 23 May 31 18:48 data -> /data/ST_2022_1_00001_L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


SAOImage ds9

File Edit View Frame Bin Zoom Scale Color Region WCS Analysis Help
file edit view frame bin zoom scale color region wcs analysis help
contours grid block in block out block fit block 1 block 2 block 4 smooth
0.059 0.12 0.18 0.24 0.3 0.35 0.41 0.47 0.53
0.4
0.2
0

File ska_rc_demo_01.fits
Object COMA36
Value 0.421927
Physical X 1038 Y 507
Image X 1038 Y 507
Frame 1 x 1 0 °

RAP and Grouper at INAF IA2 Archive



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).

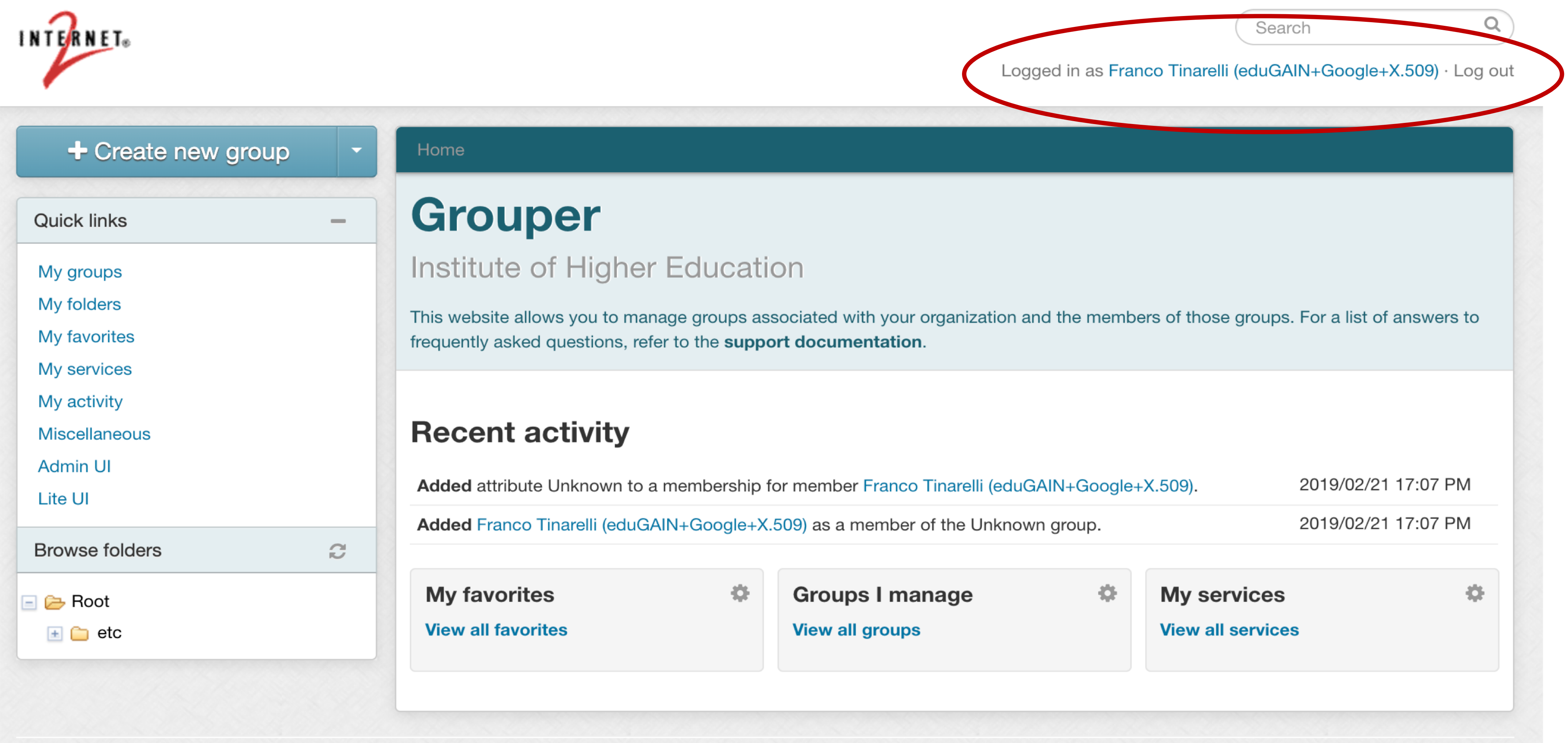
Use the IA2 Logo to Login if you have an account provided by IA2 or self registered

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



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

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

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

Thanks for your attention!

Questions?