



# AENEAS WP6

## Task 6.1

# AAI Piloting activities and deliverables

Cristina Knapic



# WP6 Objectives

Tasks	Project Objectives
<b>T6.1 Federated Authentication, Authorization Infrastructure (AAI) and Identity Provisioning (AAI)</b> <i>(Lead: INAF)</i>	<ul style="list-style-type: none"><li>• Collection of AAI Requirements</li><li>• Recommendation of approaches and solutions</li><li>• Proposal of a trust model</li></ul>



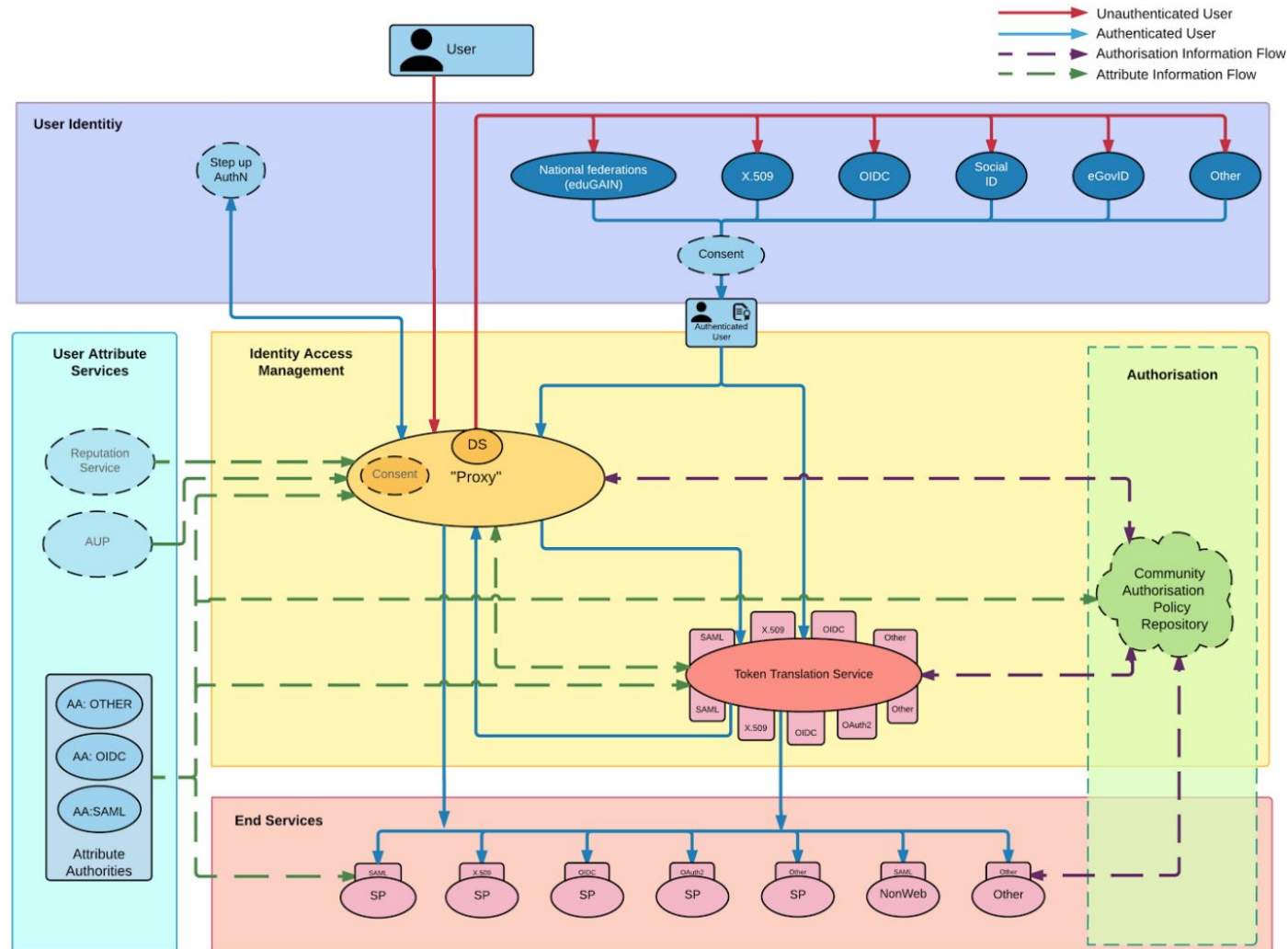
# D6.1 Activities

- Detailed analysis of the BPA architecture;
- Detailed analysis of the IVOA Authorization guidelines (recommandations);
- Revision of the mapping of AENEAS ESRCs AAI requirements to the AARC BPA at the light of new inputs from other WPs and externals;
- Detailed definition on strategies for piloting:
  - IVOA-BPA Interoperability Recommendations (inc. account linking);
  - VO RAP prototype further dev & testing;
  - Fed AAI/checkin integration with owncloud for serving data (with login/groups)
  - RCauth Testing with Grid Middleware
  - Collaboration Tools and Federated AAI Integration
- Final recommendations in D6.3.

# AARC BPA

Detailed analysis of the AARC BPA architecture highlighted the feasibility and applicability of the recommendation for infrastructures exchange of identity attributes.

Debate on the interactions between infrastructure level AAI and high level VO compliant AAI : how to be omni-comprehensive.

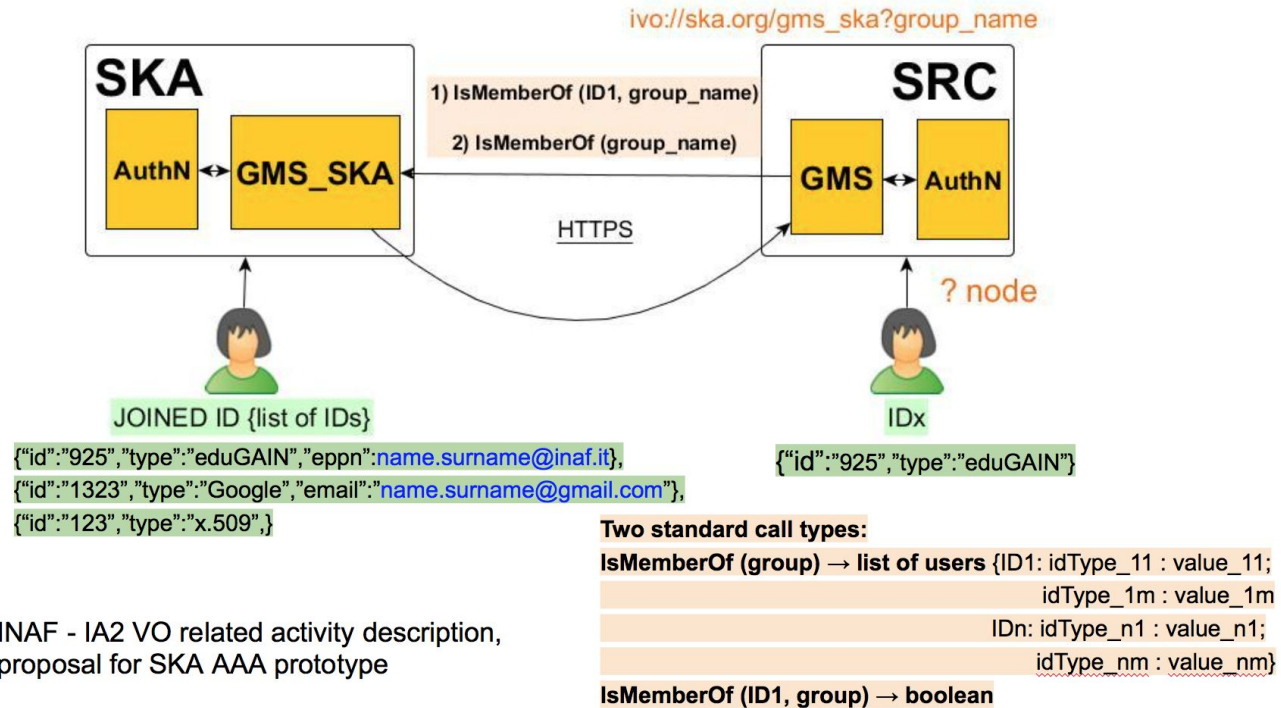


# IVOA AuthZ recommendations

Study of the IVOA standards (VOSpace and recent working draft for AuthZ) makes emerge the general approach to address also the account linking requirement. It has to be translated into OIDC token to interoperate with a BPA implementation.

## 1. Multi-protocol AuthN - 2) Account Linking

Courtesy of C. Knapic - G. Jerse -- INAF - OATs



INAF - IA2 VO related activity description, proposal for SKA AAA prototype

# Requirements specification document

Table 1: List of general functional requirements, relative descriptions and mapping to AARC resources.

Req #	Description	Recommendation resource(s)
Func1	Roles include Project Investigator (PI) and project group member	<ul style="list-style-type: none"> <li>VO Platforms for Research Collaboration (<a href="#">DJRA1.3</a>)</li> <li>Expressing group membership and role information (<a href="#">AARC-G002</a>)</li> </ul>
Func2	SKA AAA system shall provide an Authorization service to handle the creation and management of groups and subgroups	<ul style="list-style-type: none"> <li>Authorisation across multi-SP environments (<a href="#">Draft AARC-I047</a>)</li> <li>Expressing group membership and role information (<a href="#">AARC-G002</a>)</li> <li>Expressing resource capabilities (<a href="#">AARC-G027</a>)</li> </ul>
Func3	A PI can retrieve data for an observed proposal and administer its project group (add/delete new collaborators)	<ul style="list-style-type: none"> <li>VO Platforms for Research Collaboration (<a href="#">DJRA1.3</a>)</li> </ul>
Func4	A PI should be recognized by the same credentials from the proposal submission up to advanced products generation at SRC. The authorizations should be propagated.	<ul style="list-style-type: none"> <li>Account linking and LoA elevation use cases and common practices for international research collaboration (<a href="#">AARC-G009</a>)</li> </ul>
Func5	A PI can be a PI for different project proposals	<ul style="list-style-type: none"> <li>VO Platforms for Research Collaboration (<a href="#">DJRA1.3</a>)</li> <li>Expressing group membership and role information (<a href="#">AARC-G002</a>)</li> </ul>
Func6	A PI can be Co-I for different proposals	<ul style="list-style-type: none"> <li>VO Platforms for Research Collaboration (<a href="#">DJRA1.3</a>)</li> <li>Expressing group membership and role information (<a href="#">AARC-G002</a>)</li> </ul>
Func7	An SRC staff member assigned to an observed proposal (ARC-like "contact scientist") can access the PI data with some administrative privileges over the PI himself/herself	<ul style="list-style-type: none"> <li>VO Platforms for Research Collaboration (<a href="#">DJRA1.3</a>)</li> <li>Expressing group membership and role information (<a href="#">AARC-G002</a>)</li> </ul>

A detailed analysis of both already identified and new requirements coming from other AENEAS WP deliverables and from improvements in international standards was done. In the D6.3, the new mapping between requirements and responses will be reported. It will be updated at the light the final suggestions emerging from the incoming work of AENEAS teams by the end of month 36.

# Piloting activities

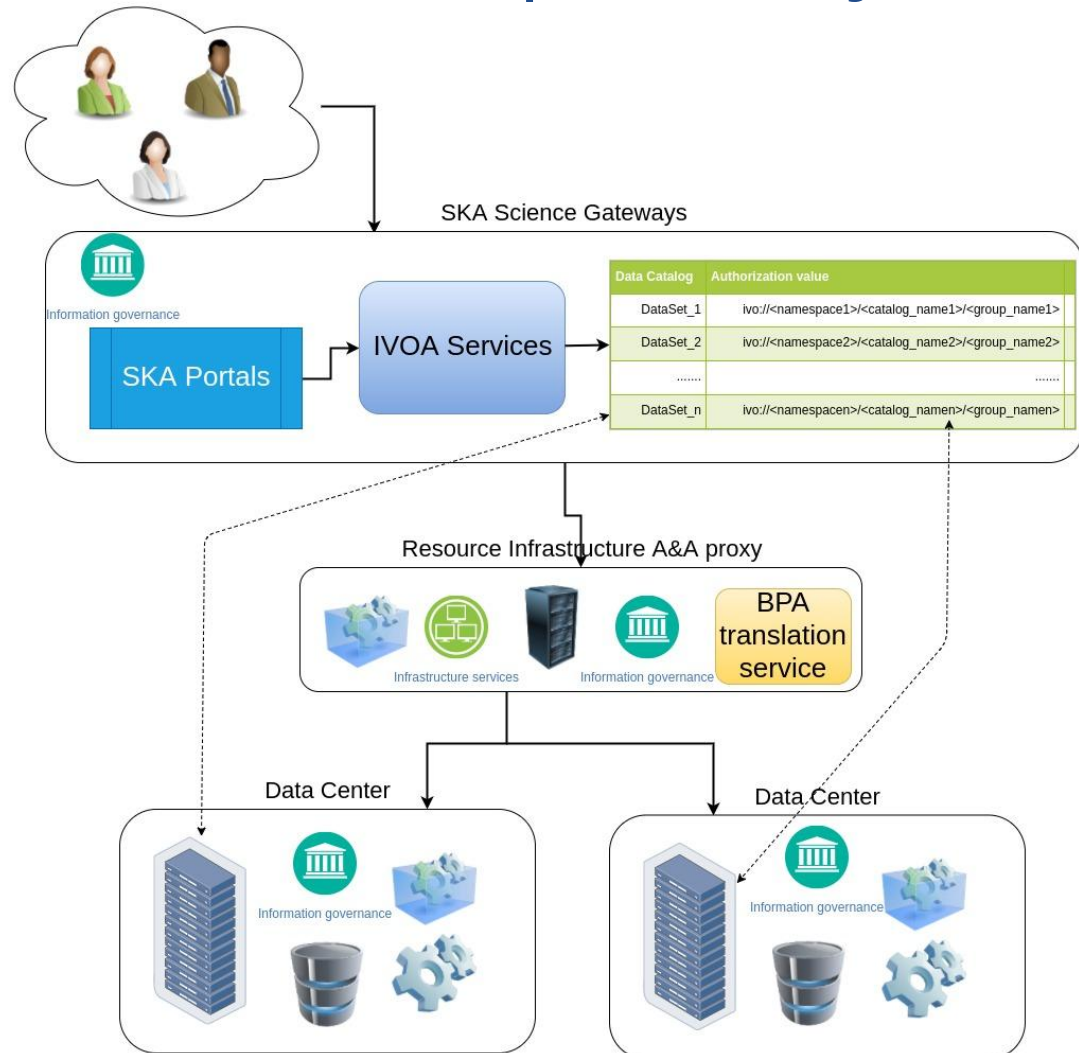
In order to verify the feasibility of all the architectures and designs proposed, a list of pilots was defined. At the beginning 7 pilots were identified, while some of them confluenced into others. Here a scratch of them:

- **Activity #1 - IVOA-BPA Interoperability Recommendations (inc. account linking):** in order to harmonize the requirements of having a VO compatible services and a BPA compliant infrastructure, we plan to develop a test science gateway VO compatible and integrate the BPA architecture in order to allow the execution of both VO compatible services calls as well as computation in a distributed (and possibly not VO compliant) environments
- **Activity #2 - INAF VO RAP prototype further dev & testing:** The use case consists of a user that using a Proposal Id would like to access his/her data in a workspace capable to give access to computational resources. It simulate the science gateway and the redirection to the data lake where data can be found
- **Activity #3 - Fed AAI/checkin integration with (INAF) Owncloud for serving data (with login/groups):** provision a second test instance of Owncloud, linked with EGI Check-In, to demonstrate federated AAI and serve data requiring group-based authentication (e.g. to a group of researchers) and data accessible to only one person (e.g. to demonstrate embargoed data);
- **Activity #4 - AAI piloting as part of science data challenges with eInfastructures - now closed as it's being covered in # 3;**
- **Activity # 5 - AAI piloting as part of itsm tools with eInfastructures (Close as part of #7)**
- **Activity # 6 - RCauth Testing with Grid Middleware:** Investigate the feasibility of having users use RFC3820 proxy certificates from the RCauth online CA for interacting with grid storage elements, leveraging the possibilities provided by Dirac. Ideally Dirac should be adapted so that users can do all work via the webportal and don't need any proxy certificate on the cmdline;
- **Activity #7 - Collaboration Tools and Federated AAI Integration:** To pilot common tools in a federated environment, e.g. wikis, mailing lists, and planning/registrations. In extension, we want to make the community get used to the federated way of working.



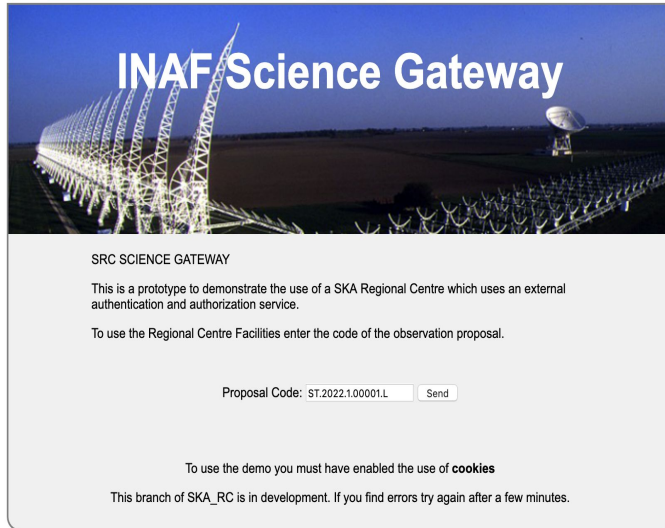
# #1 IVOA - BPA interoperability

Depending on infrastructure features, the BPA as well as the IVOA recommendations should be supported. Here a draft architecture that can respond to both requirements:

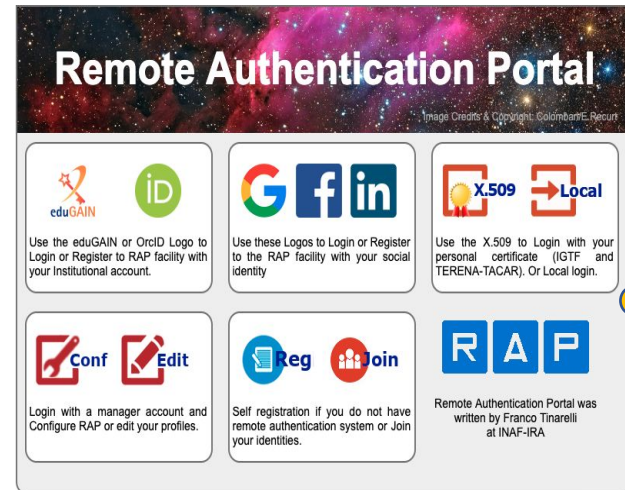




# #1 IVOA - BPA interoperability



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



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

**Grouper/GMS**  
 IN: groupID, user\_unique\_ID  
 OUT: authorization

IN:  
 Authentication  
 OUT: User  
 Unique ID

# #1 IVOA - BPA interoperability



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](#)

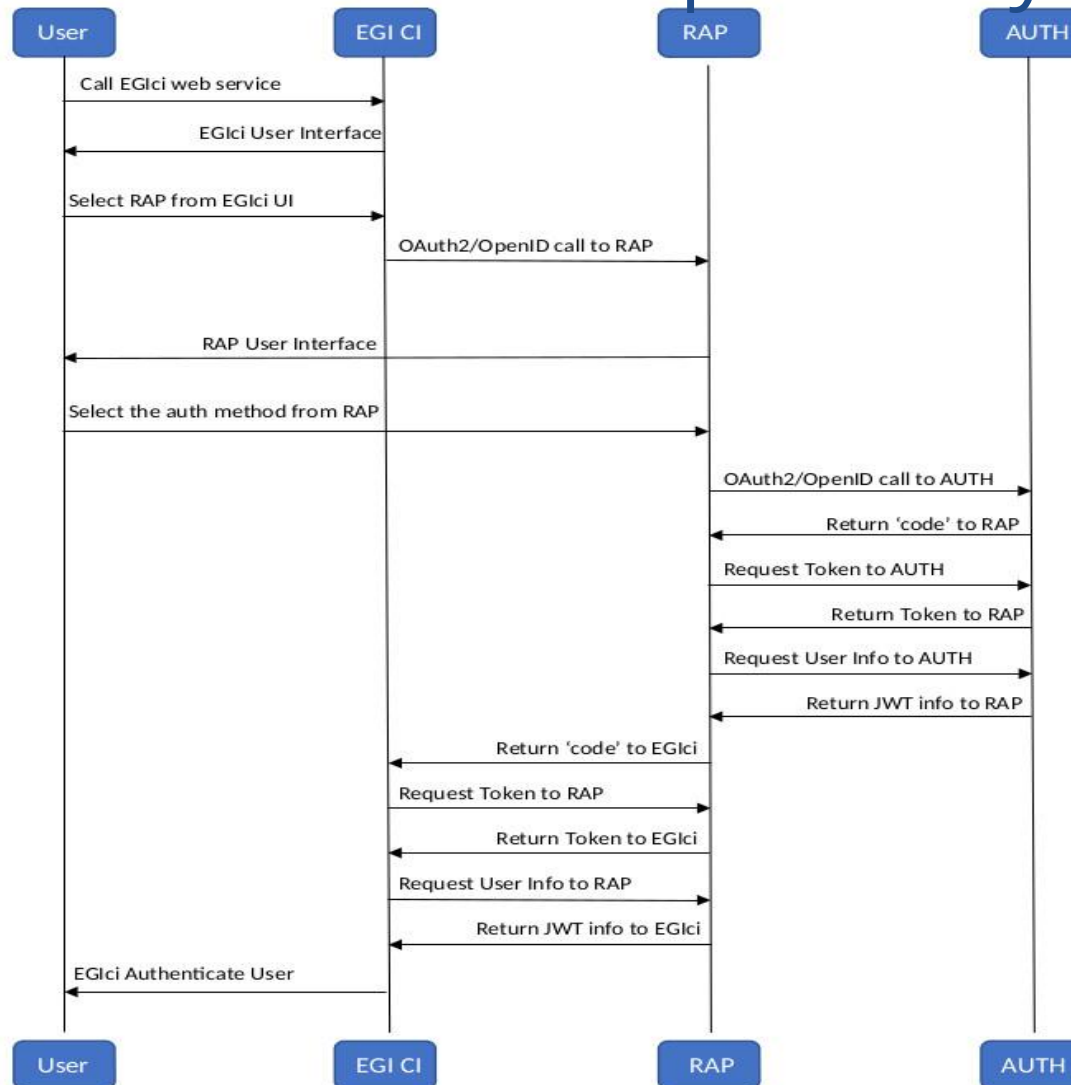
### Groups I manage

[View all groups](#)

### My services

[View all services](#)

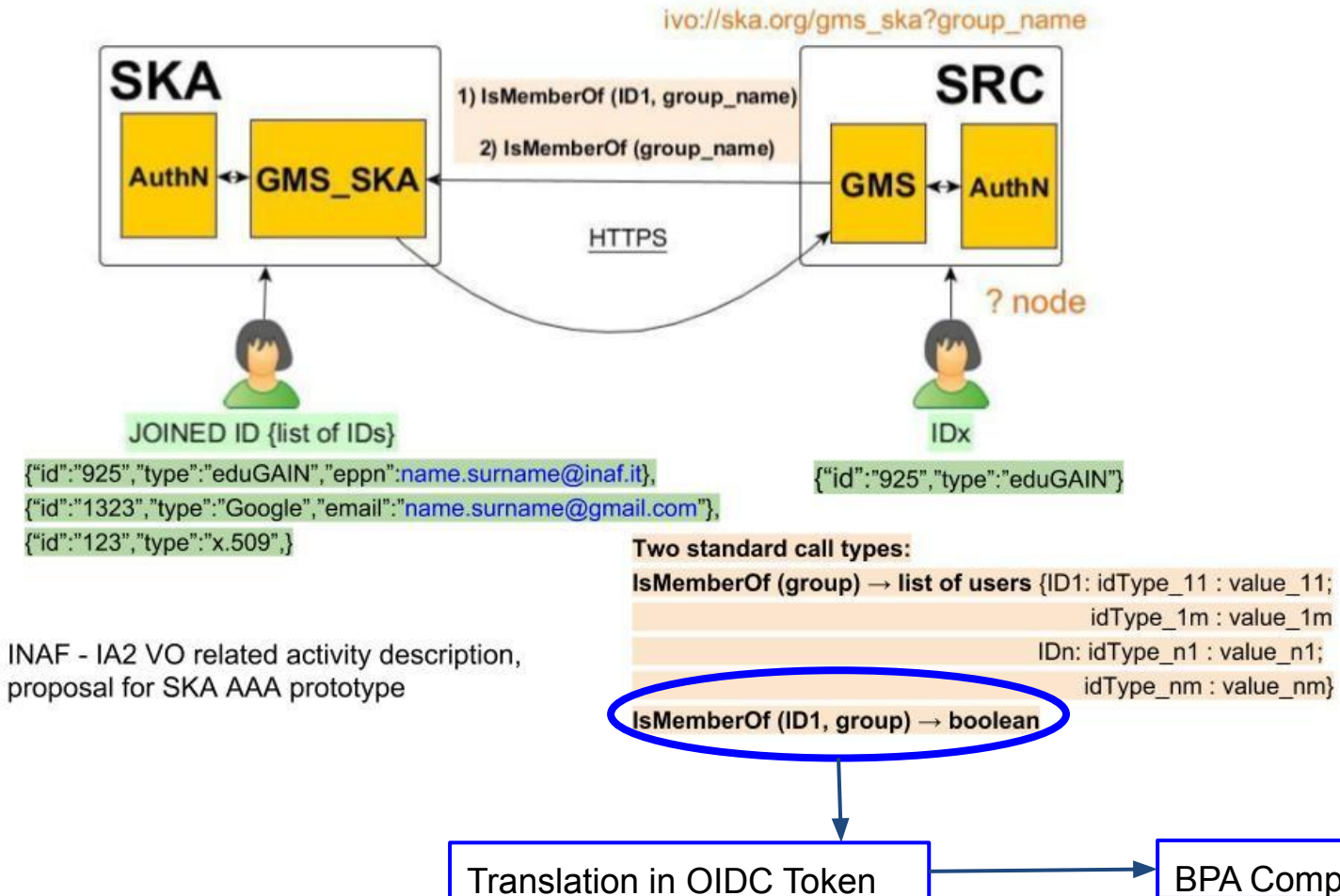
# #1 IVOA - BPA interoperability



# #1 IVOA - BPA interoperability

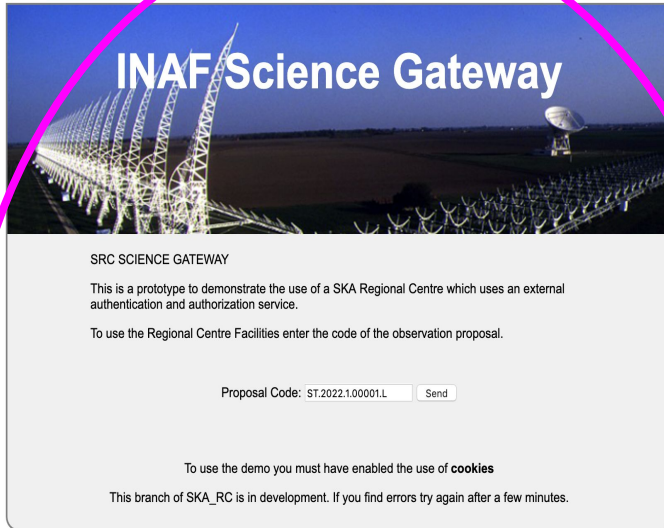
## 1. Multi-protocol AuthN - 2) Account Linking

Courtesy of C. Knapic - G. Jerse -- INAF - OATs




INAF - IA2 VO related activity description,  
proposal for SKA AAA prototype

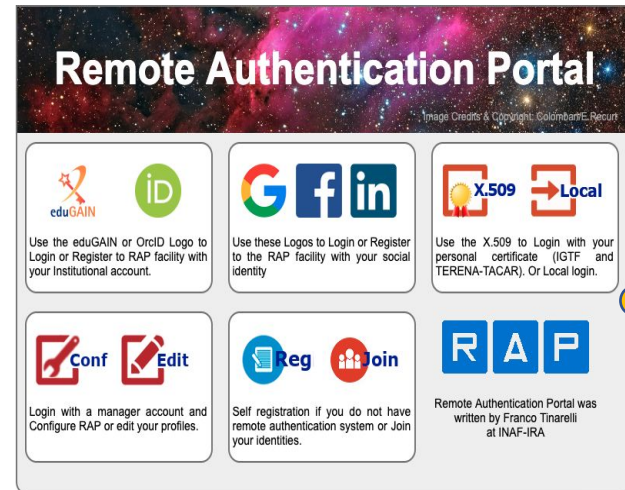
# #2 RAP devels



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




**Remote Authentication Portal**



RAP

**Grouper/GMS**  
 IN: groupID, user\_unique\_ID  
 OUT: authorization

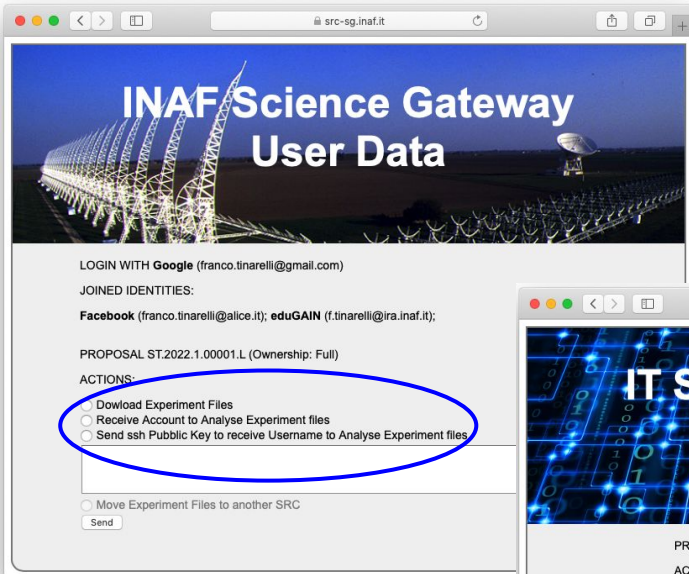


**Data Center  
 (Archive+Computation)**  
 Token exchange  
 Data access and computation

IN:  
 Authentication  
 OUT: User  
 Unique ID



# #2 RAP devels



INAF Science Gateway  
User Data

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

JOINED IDENTITIES:

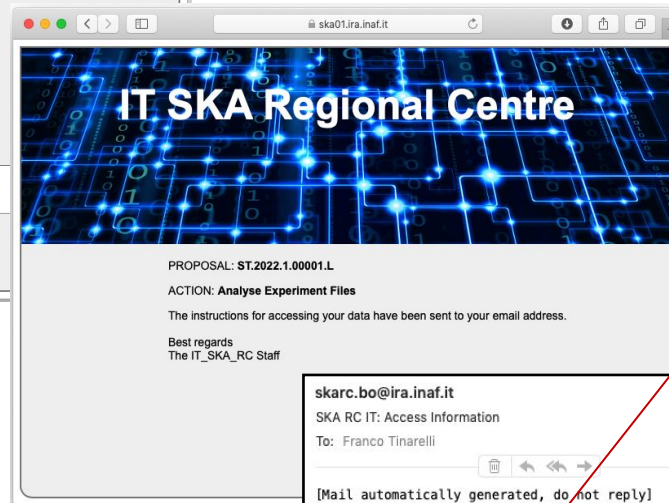
**Facebook** (franco.tinarelli@alice.it); **eduGAIN** (f.tinarelli@ira.inaf.it);

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



IT SKA Regional Centre

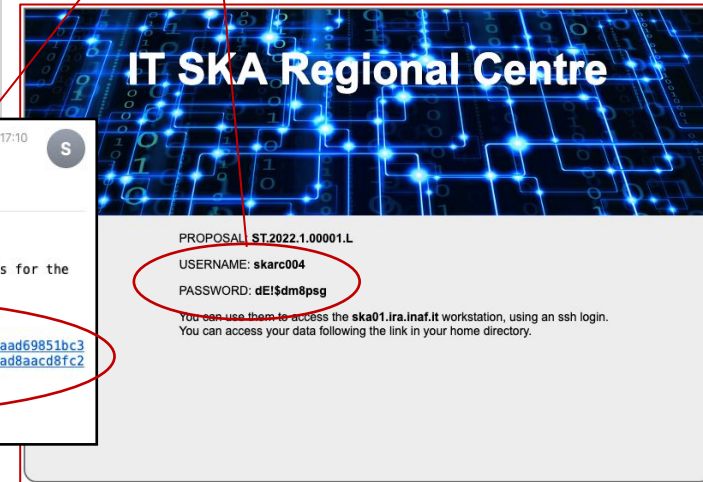
PROPOSAL: ST.2022.1.00001.L

ACTION: **Analyse Experiment Files**

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

Best regards  
The IT\_SKA\_RC Staff

Obtain an account to  
analyze your data



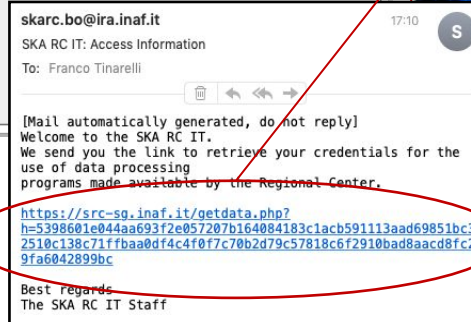
IT SKA Regional Centre

PROPOSAL: ST.2022.1.00001.L

USERNAME: **skarc004**

PASSWORD: **dEi\$dm8psg**

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.



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

SKA RC IT: Access Information

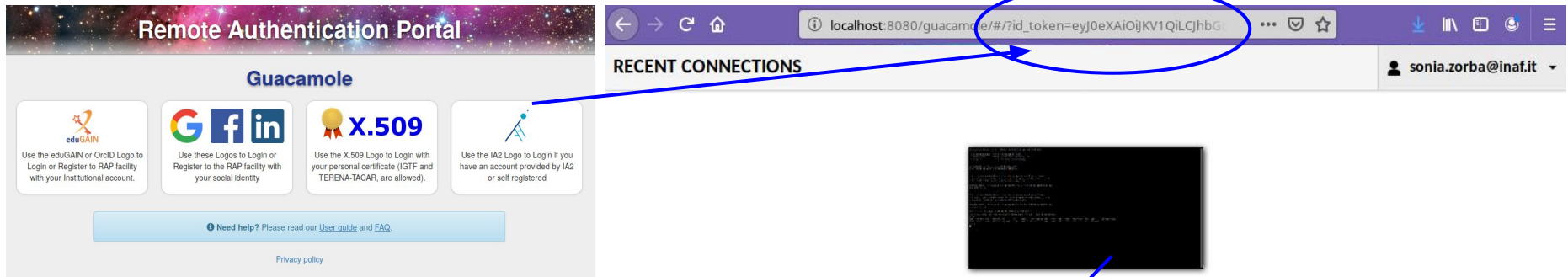
To: Franco Tinarelli

[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.

<https://src-sg.inaf.it/getdata.php?h=5398601e044aa693f2e057207b164084183c1acb591113aad69851bc32510c138c71ffbaa0df4c4f0f7c70b2d79c57818c6f2910bad8aacd8fc29fa6042899bc>

Best regards  
The SKA RC IT Staff

# #2 RAP devels

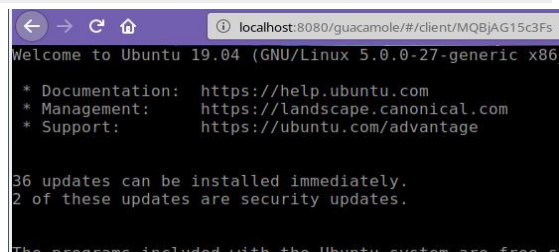


Remote Authentication Portal

Guacamole

RECENT CONNECTIONS

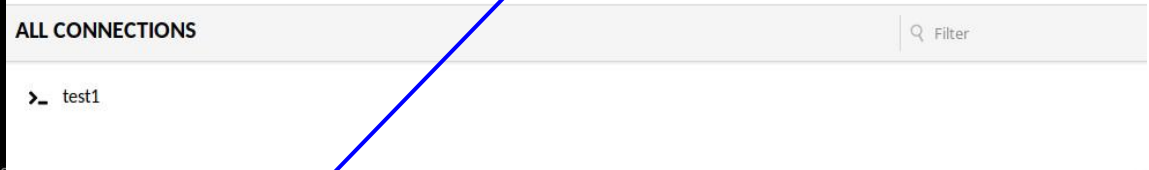
sonia.zorba@inaf.it



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

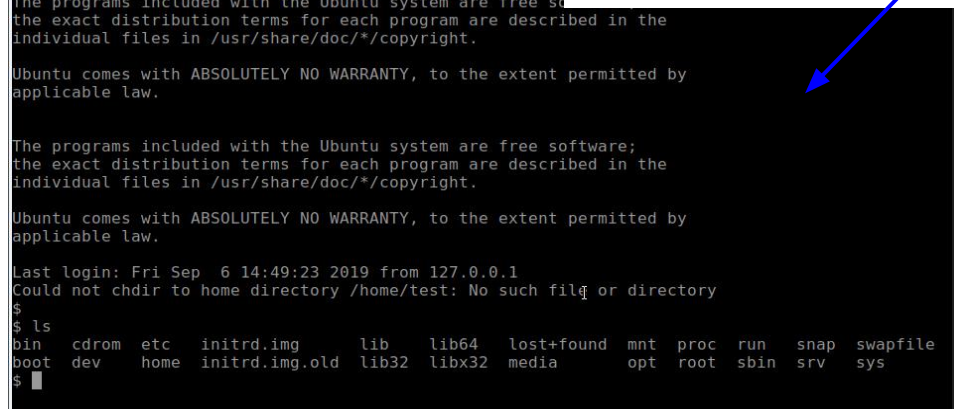
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

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



ALL CONNECTIONS

test1



```

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.

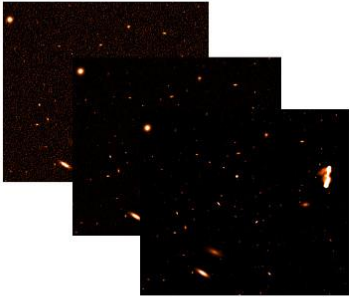
Last login: Fri Sep  6 14:49:23 2019 from 127.0.0.1
Could not chdir to home directory /home/test: No such file or directory
$
$ ls
bin  cdrom  etc  initrd.img  lib  lib64  lost+found  mnt  proc  run  snap  swapfile
boot  dev  home  initrd.img.old  lib32  libx32  media  opt  root  sbin  srv  sys
$
```

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



# #3 Egi -CheckIn integration with OwnCloud

## SKA Science Data Challenge #1



The SKA Science Data Challenge #1 (SDC1) release consists of 9 files, with the format of FITS images. Each file is a simulated SKA continuum image in total intensity of the same field at 3 frequencies (560 MHz, representative of SKA Mid Band 1, 1.4 GHz, representative of SKA Mid Band 2 and 9.2 GHz, representative of SKA Mid Band 5) and 3 telescope integrations (8, 100, 1000 h as representative of a single, medium-depth and deep integration, respectively).

Ancillary data consist of primary beams and synthesized beams for each frequency. An explanatory supplement describes the data and the challenge that is set for the community. A training set is also released, which consists in truth catalogues listing the subjects in the simulated 1000 h data and their properties for a 5% of the field-of-view.

Zoom-in of the 1.4 GHz maps, showing the same region of the sky with different telescope integration: 8, 100, 1000 h left to right.

### Challenge Description

The challenge set for the community is to identify:

- source finding (RA, Dec) to locate the centroids and source positions
- source property characterization (integrated flux density, visible core fraction, major and minor axis size, major axis position angle)
- source population identification (line or SF-G, AGN-steep, AGN-flat)

The full description of the data and of the challenge set is here:  
SKA Data Challenge #1 description [DOWNLOAD](#)

Take up the challenge!



**Provision/migrate Owncloud to Nextcloud and add as a SP to the dev Check-In.**

No OIDC supported

OIDC supported



## #6 RCauth Testing with Grid Middleware

- it will provide an easy means for SKA users to interact with Grid-based storage without the need for handling certificates and their private keys;
- Check-in login to the Dirac web portal is possible now with DIRAC4EGI using OIDC and Check-In;
- Demonstrate launching of SKA workflows onto GridPP resources via RCauth without certificate.



Please ask details to Matthew, Mischa, David, Jouke, Rohini and Daniele



## #7

- Knowledge transfer of the AARC BPA to the SDC team at ASTRON;
- Exploration of potential implementations
- Implementation of the AAI infrastructure;
- Linking arbitrary services to the AAI infra;
- ASTRON now has some experience with linking federated services

# ASTRON

Netherlands Institute for Radio Astronomy

Please ask details to Matthew, Jouke and Zheng



# Final recommendations

All the activities results are under reporting into the final deliverable due on Month 36.

Most of the recommendations were summarized here to complete the previous deliverable content.

**Thank you !**