AENEAS WP6
Task 6.1
AAI Piloting activities and deliverables

Cristina Knapic

WP6 Objectives

Tasks	Project Objectives
T6.1 **Federated Authentication, Authorization Infrastructure (AAI) and Identity Provisioning** (AAI) *(Lead: INAF)*	• Collection of AAI Requirements • Recommendation of approaches and solutions • Proposal of a trust model

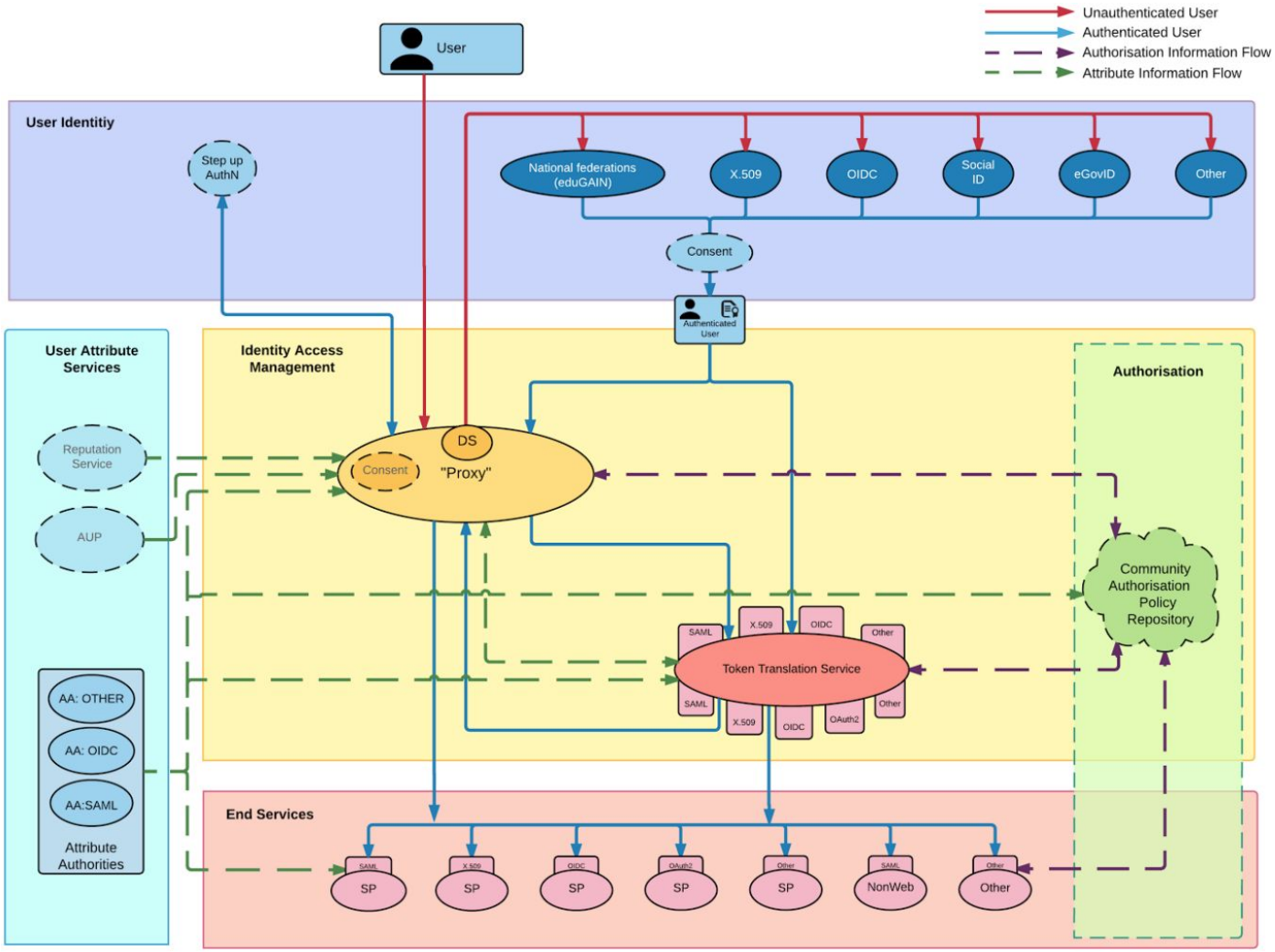
D6.1 Activities

- 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.

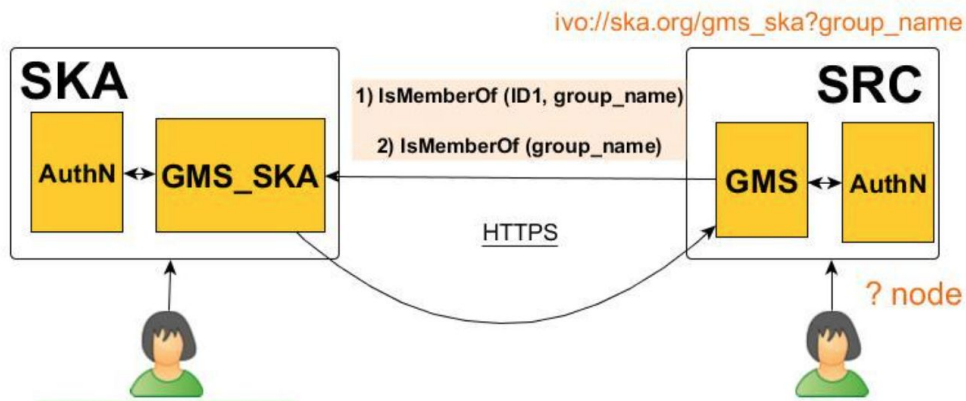


IVOA AuthZ recommendations

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



JOINED ID {list of IDs}

{"id":"925","type":"eduGAIN","eppn":name.surname@inaf.it},
{"id":"1323","type":"Google","email":"name.surname@gmail.com"},
{"id":"123","type":"x.509",}

IDx

{"id":"925","type":"eduGAIN"}

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

Two standard call types:

IsMemberOf (group) → list of users {ID1: idType_11 : value_11;
idType_1m : value_1m
IDn: idType_n1 : value_n1;
idType_nm : value_nm}

IsMemberOf (ID1, group) → boolean

Requirements specification document

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.

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	• VO Platforms for Research Collaboration (DJRA1.3) • Expressing group membership and role information (AARC-G002)
Func2	SKA AAA system shall provide an Authorization service to handle the creation and management of groups and subgroups	• Authorisation across multi-SP environments (Draft AARC-I047) • Expressing group membership and role information (AARC-G002) • Expressing resource capabilities (AARC-G027)
Func3	A PI can retrieve data for an observed proposal and administer its project group (add/delete new collaborators)	• VO Platforms for Research Collaboration (DJRA1.3)
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.	• Account linking and LoA elevation use cases and common practices for international research collaboration (AARC-G009)
Func5	A PI can be a PI for different project proposals	• VO Platforms for Research Collaboration (DJRA1.3) • Expressing group membership and role information (AARC-G002)
Func6	A PI can be Co-I for different proposals	• VO Platforms for Research Collaboration (DJRA1.3) • Expressing group membership and role information (AARC-G002)
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	• VO Platforms for Research Collaboration (DJRA1.3) • Expressing group membership and role information (AARC-G002)

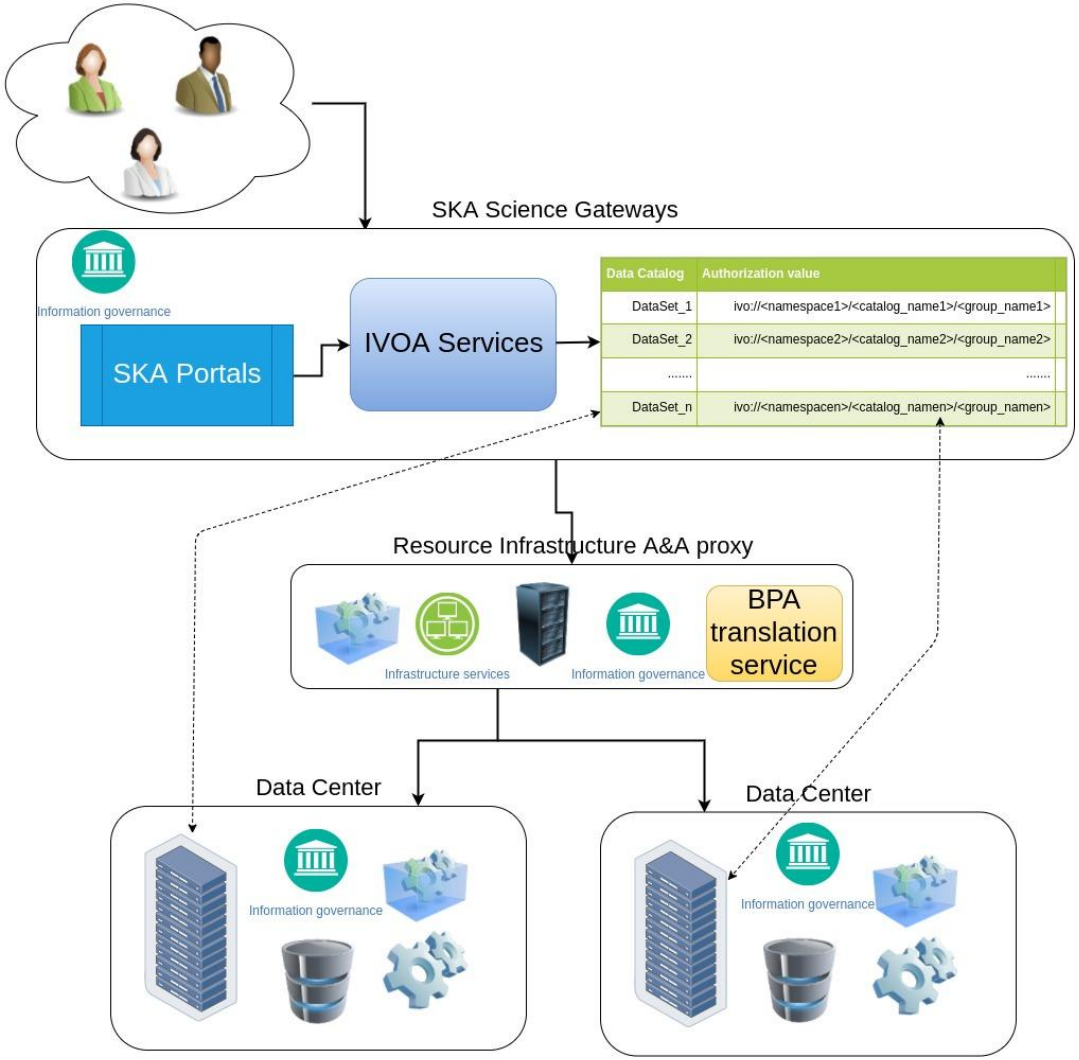
Piloting activities

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

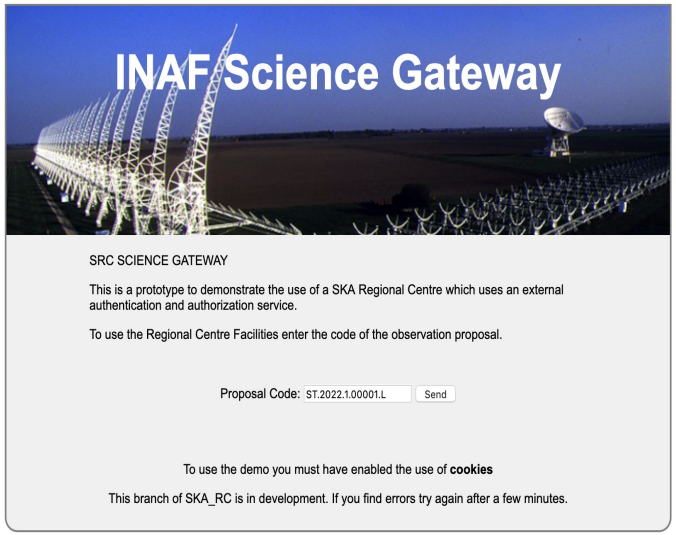
- Activity #1 - IVOA-BPA Interoperability Recommendations (inc. account linking): in order to harmonize the requirements of having a VO compatible services and a BPA compliant infrastructure, we plan to develop a test science gateway VO compatible and integrate the BPA architecture in order to allow 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 eInfrastructures - now closed as it's being covered in # 3;
- Activity # 5 - AAI piloting as part of itsm tools with eInfrastructures (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:



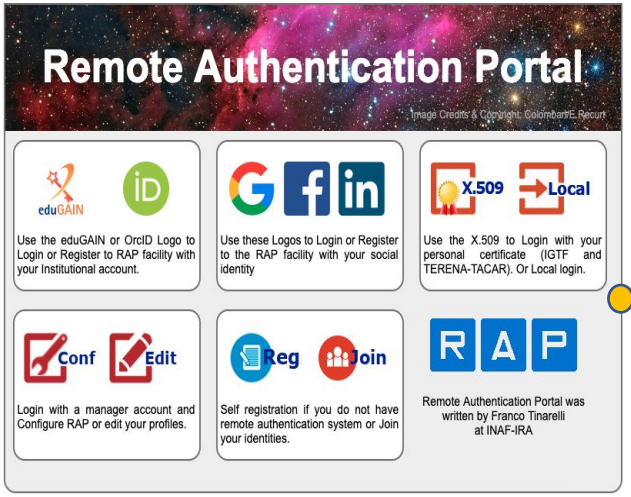
#1 IVOA - BPA interoperability



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

IN: Authentication

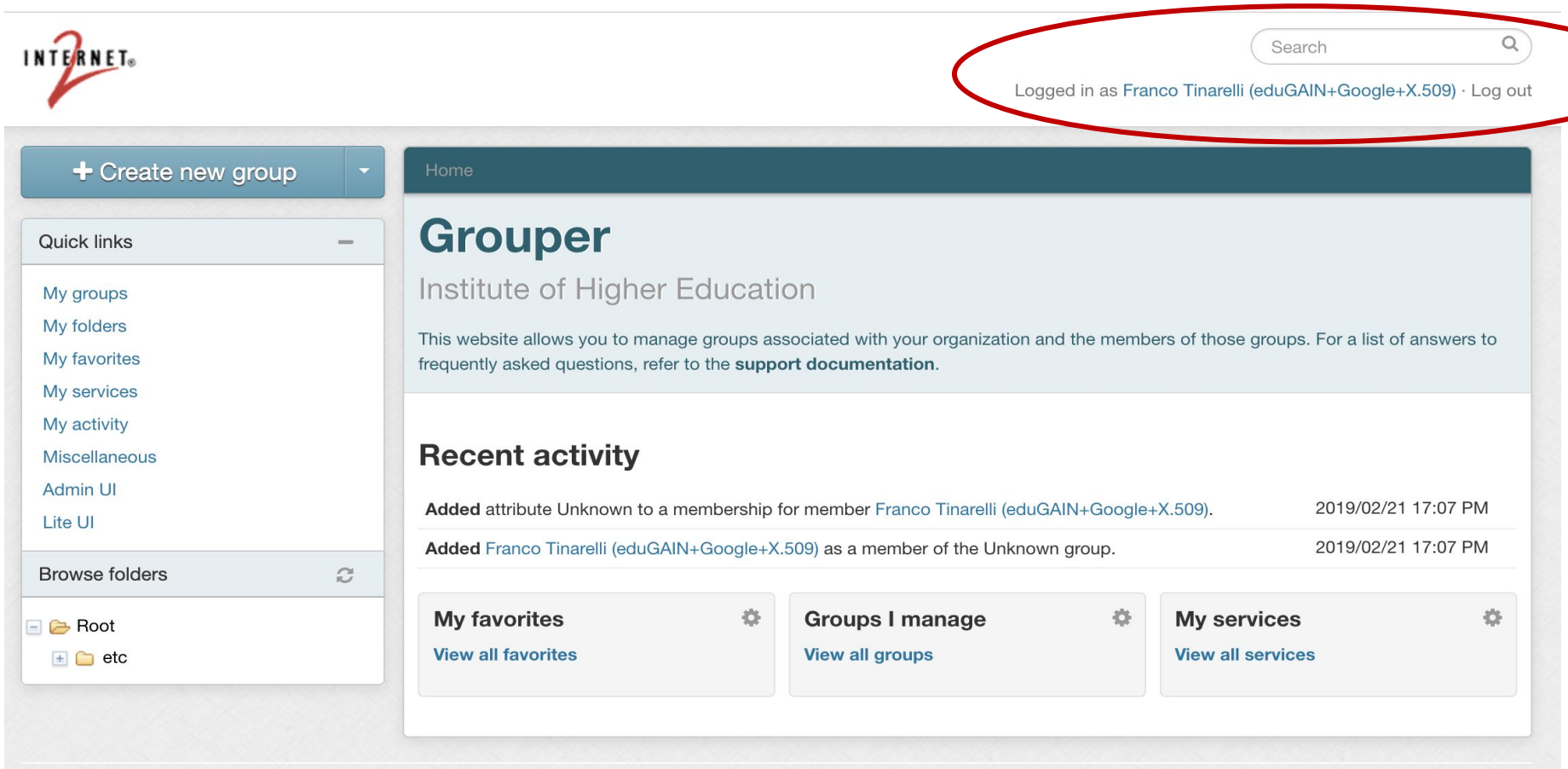
OUT: User Unique ID



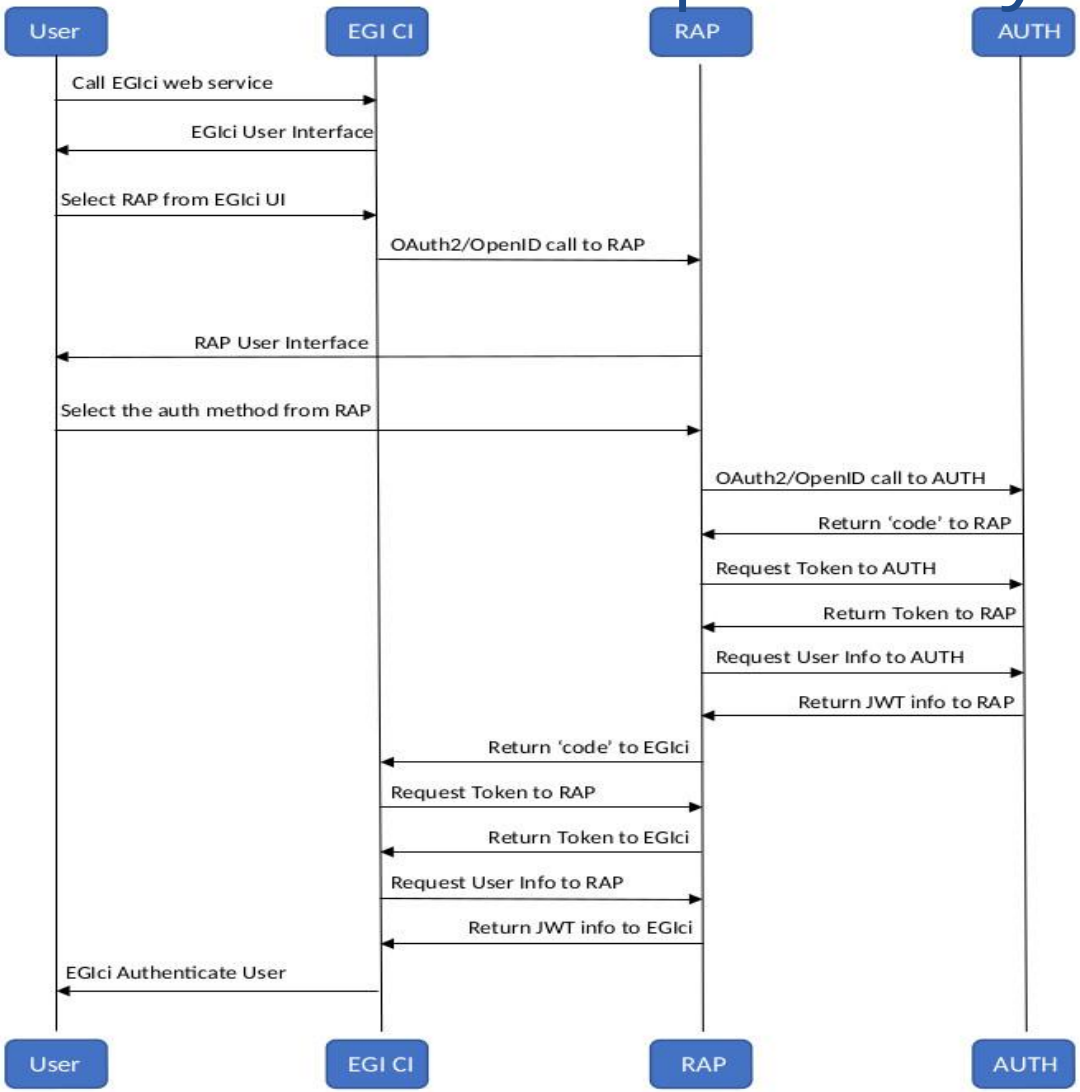
Data Center (Archive+Computation)
Token exchange
Data access and computation

Grouper/GMS
IN: groupID, user_unique_ID
OUT: authorization

#1 IVOA - BPA interoperability



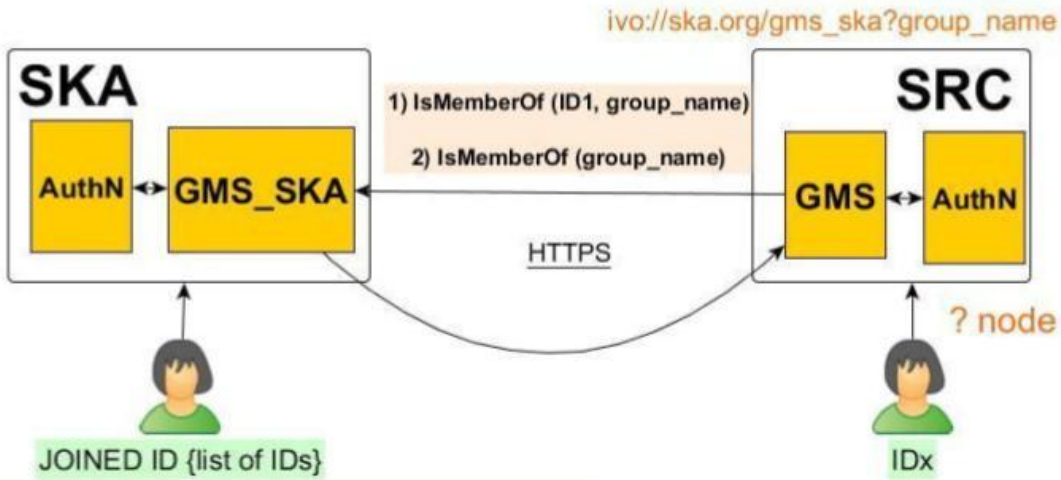
#1 IVOA - BPA interoperability



#1 IVOA - BPA interoperability

1. Multi-protocol AuthN - 2) Account Linking

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



{"id":"925","type":"eduGAIN","eppn":name.surname@inaf.it},
{"id":"1323","type":"Google","email":"name.surname@gmail.com"},
{"id":"123","type":"x.509",}

{"id":"925","type":"eduGAIN"}

Two standard call types:

IsMemberOf (group) → list of users {ID1: idType_11 : value_11;
idType_1m : value_1m
IDn: idType_n1 : value_n1;
idType_nm : value_nm}

IsMemberOf (ID1, group) → boolean

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

Translation in OIDC Token → BPA Compliancy

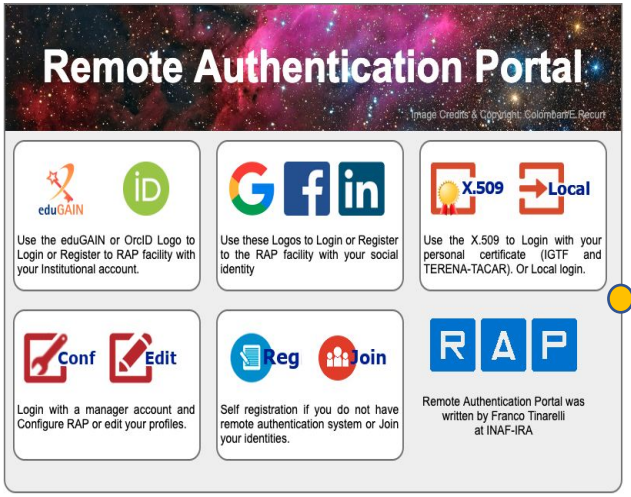
#2 RAP devels

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

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

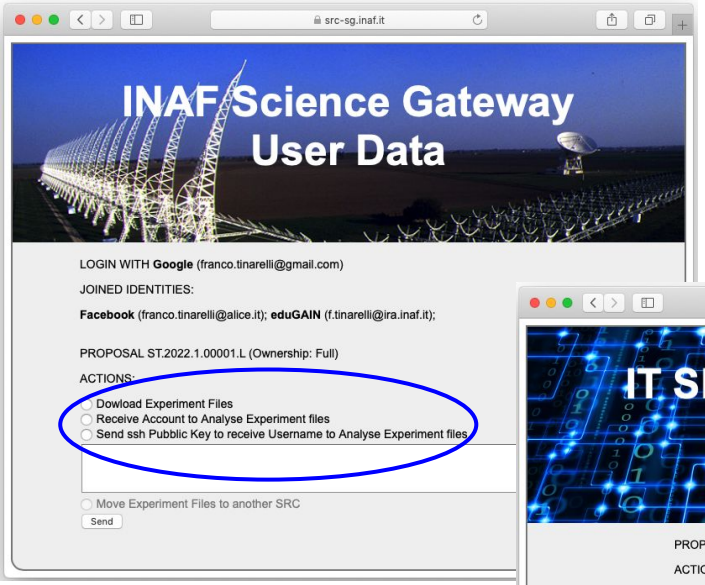
IN: Authentication

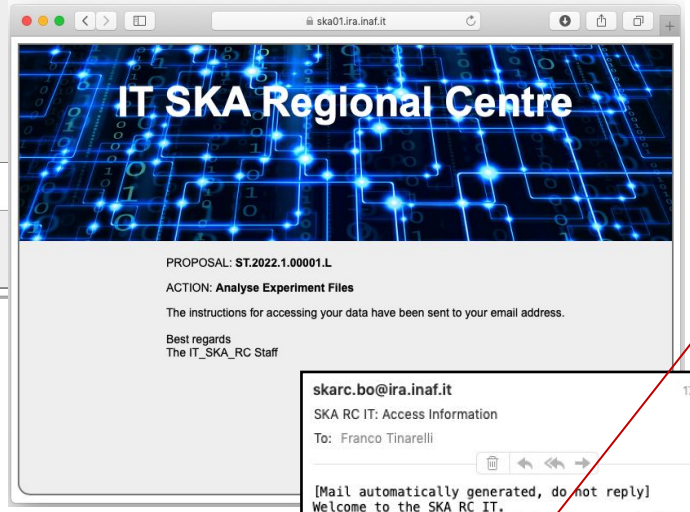
OUT: User Unique ID

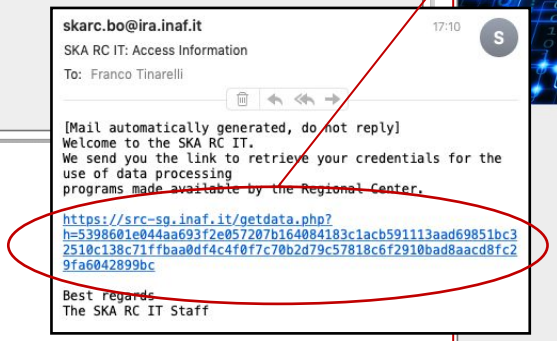


Grouper/GMS
IN: groupID, user_unique_ID
OUT: authorization

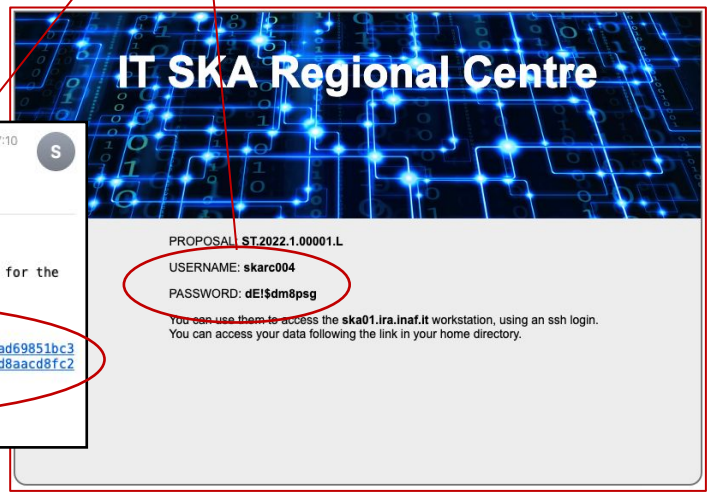
#2 RAP devels



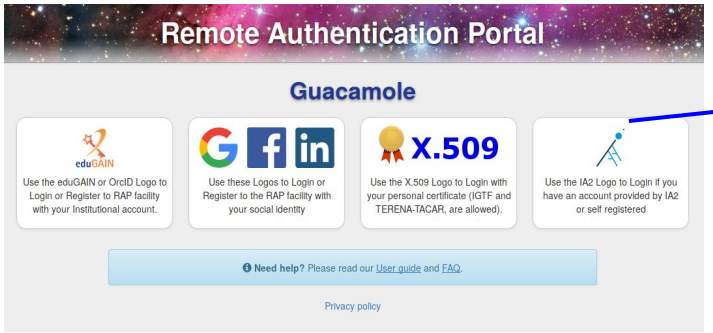


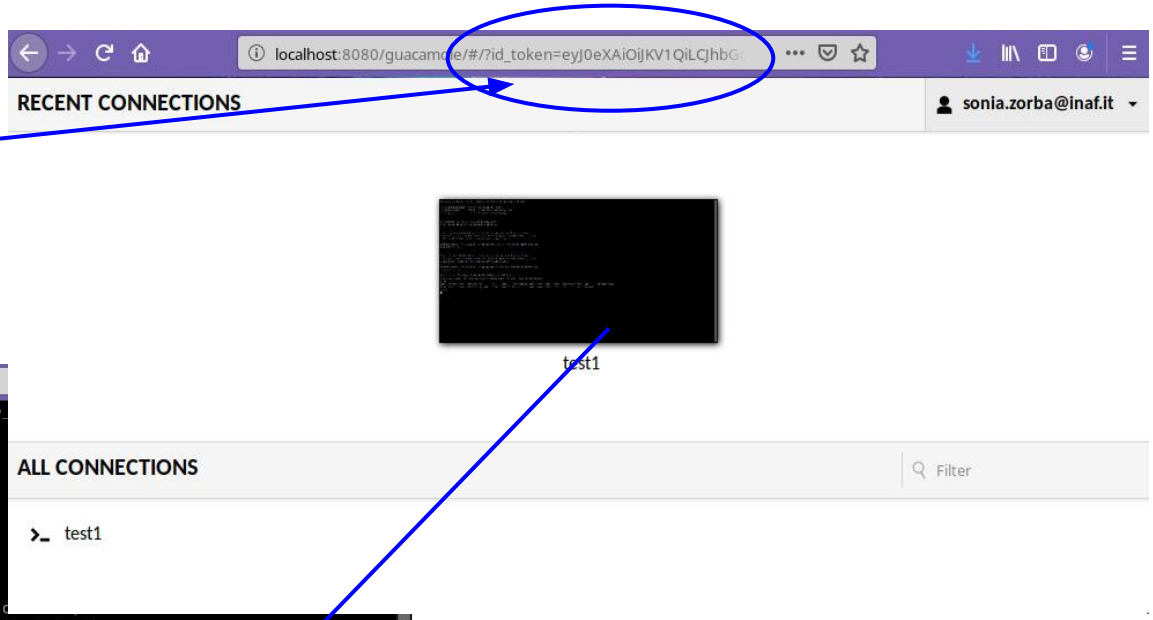


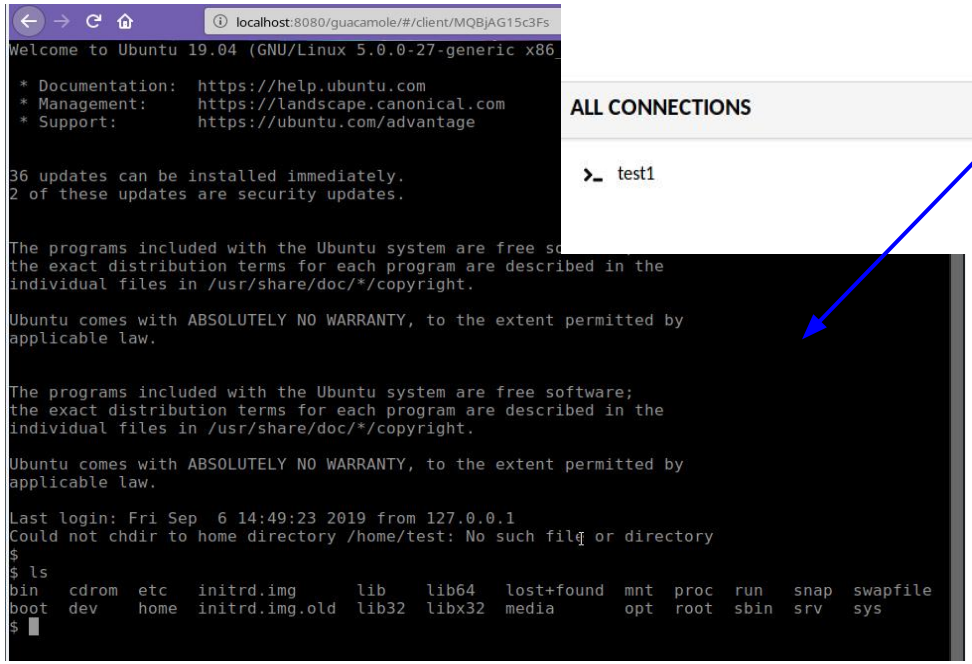
Obtain an account to analyze your data



#2 RAP devels



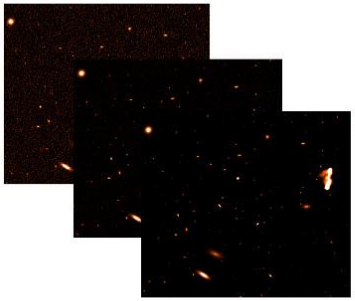




Web oriented connection using several protocols like ssh, VNC, telnet…..

#3 Egi -CheckIn integration with OwnCloud

SKA Science Data Challenge #1



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.

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 objects in the simulated 1000 h data and their properties for a 5° of the field-of-view.

Challenge Description

The challenge set for the community is to identify:

- source finding (RA, Dec) to locate the centroids and/or accurate positions
- source property characterization (integrated flux density, possible core fraction, major and minor axis size, major axis position angle)
- source population identification (one of SFG, AGN-steep, AGN-flat)

The full descritpion 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.

OIDC supported

No 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.

DIRAC
THE INTERWARE

SCIENTIFIC DATA MANAGEMENT
RUCIO

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 !