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

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

Remote Authentication Portal

IN: Authentication
OUT: User Unique ID

Grouper/GMS
IN: groupID, user_unique_ID
OUT: authorization

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
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

<table>
<thead>
<tr>
<th>Instrument</th>
<th>Year</th>
<th>Cycle</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST.2022.1.00001.L</td>
<td></td>
<td></td>
<td>ALMA syntax</td>
</tr>
</tbody>
</table>

---

**INAF Science Gateway**

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 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)

- 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.
Proxy between applications and identity providers or local registration

- 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

Authentication Methods
- edugain: True/False
- x509: True/False
- local: True/False
- google: True/False
- linkedin: True/False
- register: True/False
- join: True/False
- sql: True/False

Registration Methods
- ldap: True/False
- mariadb: True/False

Supported providers can be chosen through configuration command or editing file.

- 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
Actors: RAP the Config Command

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

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

PROPOSAL: ST.2022.1.00001.L
ACTION: Download Experiment Files

- ska_rc_demo_01.fits, Size: 8527680 byte
- ska_rc_demo_02.fits, Size: 1126080 byte
The Prototype Step by Step (4.2)

Obtain an account to analyze your data

---

**Proposal:** ST.2022.1.00001.L
**Action:** Analyse Experiment File

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

Best regards,
The IT_SKA_RC Staff

---

**Username:** skarc004
**Password:** dl15dmpwpsg

You can use these 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)

Login to computing element and analyze data.
Login without password and analyze data

```
mambo:~ ftinarei$ ssh -Y skarco04@skao01.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
[skarco04@skao01 ~]$ ls -l
total 0
lrwxrwxrwx 1 skarco04 srsusers 23 May 31 18:48 data -> /data/ST_2022_1_00001_L
[skarco04@skao01 ~]$ ls data
skar_rc_demo_01.fits skar_rc_demo_02.fits
[skarco04@skao01 ~]$ cd data
[skarco04@skao01 data]$ ls
skar_rc_demo_01.fits skar_rc_demo_02.fits
[skarco04@skao01 data]$ ds9 ska_rc_demo_01.fits
```
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

Using the two modified connectors, grouper receives the joined identities (Account Linking) from RAP.
RAP and Guacamole (courtesy of Sonia Zorba)

Web oriented connection using several protocols like ssh, VNC, telnet.....
Thanks for your attention!

Questions?