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

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

INAF Science Gateway

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

Remote Authentication Portal
IN: Authentication
OUT: User Unique ID

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

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:** ALMA

**Proposal Code:** 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
```

```java
(ivo://auth.ska.org/grouper?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).
- RAP uses OAuth2 and OpenID Connect to communicate with the Science Portal or other clients.

(Use the link [https://rap.inaf.it/Services/RAP](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.
Actors: RAP and the Customization

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

```javascript
$SKA = array (...,
    'eduGain' => true,
    'orcid' => false,
    'x509' => true,
    'local' => false,
    'google' => true,
    'facebook' => false,
    'linkedIn' => false,
    'useldap' => true,
    'edit' => true,
    'register' => false,
    'join' => true,
    'edit' => true,
    ... );
```

Each application that uses RAP can declare which functions are enabled among the declared ones. The table below shows which options are enabled; you can change them in the `users.rap.conf` file to see which happens in RAP. Be careful that if you do not use LDAP and Mercurial, join and edit functions will be ignored.

Authentication Methods:
- eduGain
- OrcID
- X.509
- Local
- Google
- Facebook
- linkedIn
- USE LDAP
- USE DBMS
- EDIT
- REGISTER
- JOIN
- EDIT

Registration Methods:
- LDAP
- Mercurial
- Register
- Join
- Edit
ST_2022_1_00001_L / 10001

53330313931303232f7ce4ea1@rap.inaf.it

**Grouper/GMS**

IN: groupID, user_unique_ID

OUT: 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
```

**Authorization**
Actors: The Data Centre

- 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
The Prototype Step by Step (2)

Authenticate Yourself
The Prototype Step by Step (3)

Select the actions to manage your data
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)

Login to computing element and analyze data
The Prototype Step by Step (4.3)

Send your ssh public keys to login without password

Send

skarc.bo@ira.inaf.it
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
The Prototype Step by Step (4.3.1)

Login without password and analyze data
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.
Thanks for your attention!

Questions?