A&A @ SKA

Cristina Knapic

SKA
SQUARE KILOMETRE ARRAY

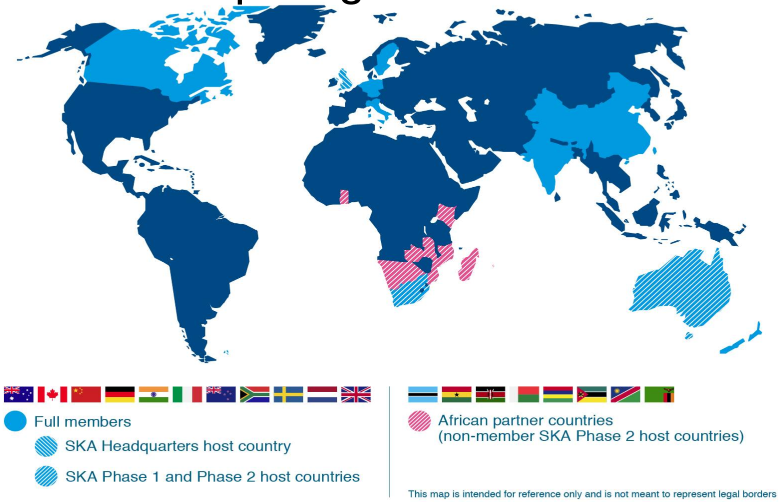
SWINBURNE ASTRONOMY PRODUCTIONS
WWW.VR.SWIN.EDU.AU

- 2020 era radio telescope
- Very large collecting area (km^2)
- Very large field of view
- Wide frequency range (70MHz - 25 GHz)
- Large physical extent (3000+ km)

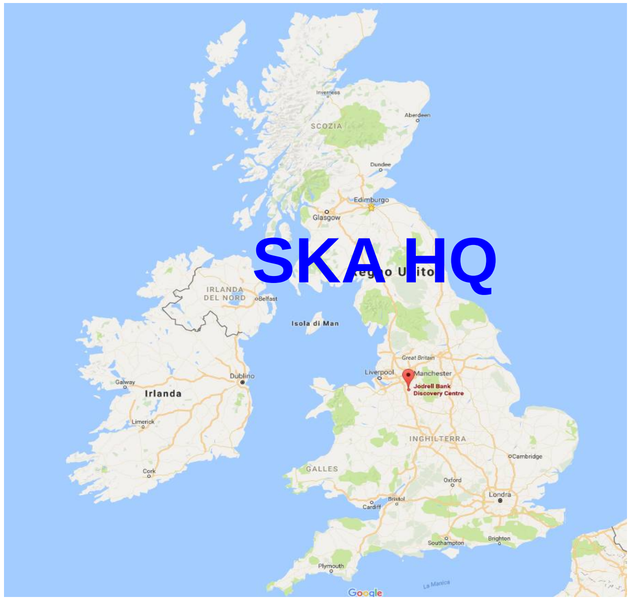
- International project
- Telescope sited in Australia and/or South Africa
- Headquarters at Jodrell Bank, UK
- Multiple pathfinders and precursors now being built around the world

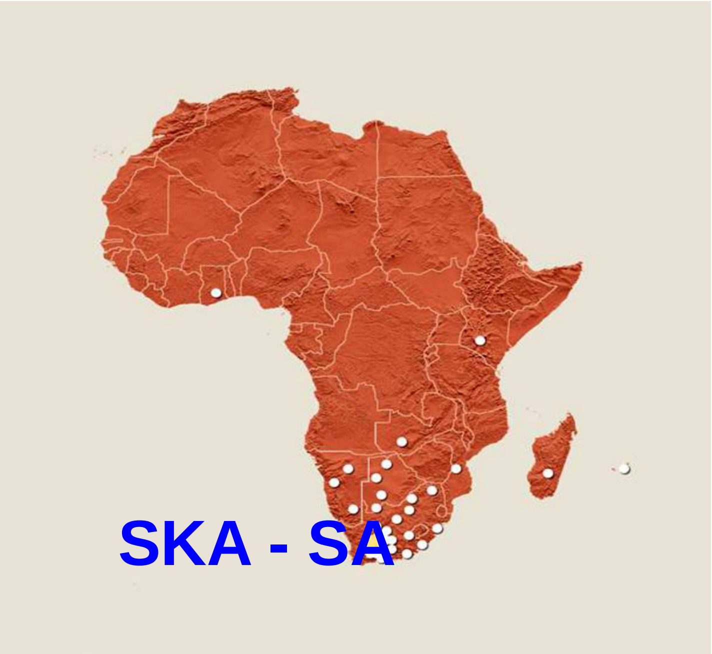
SKA Locations

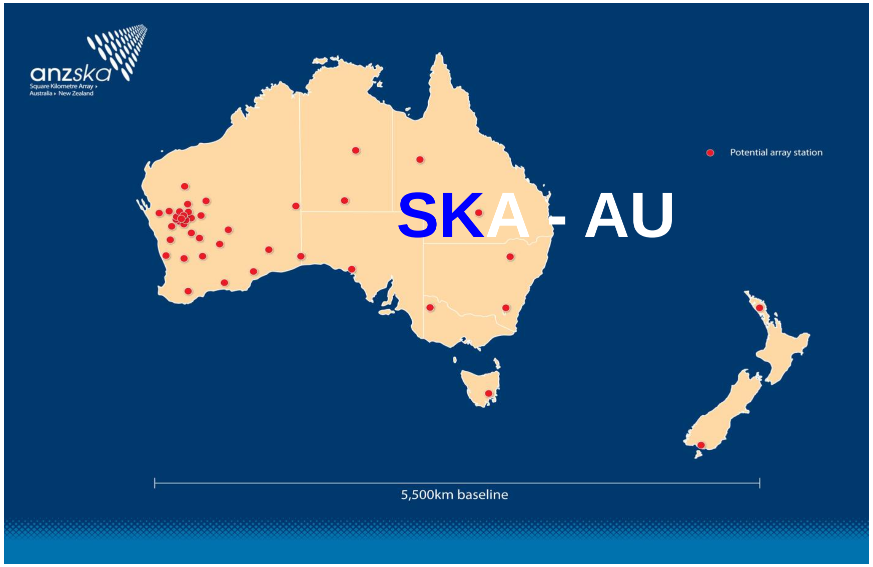
Participating countries


● Full members
▨ SKA Headquarters host country
▨ SKA Phase 1 and Phase 2 host countries
▨ African partner countries
(non-member SKA Phase 2 host countries)
This map is intended for reference only and is not meant to represent legal borders

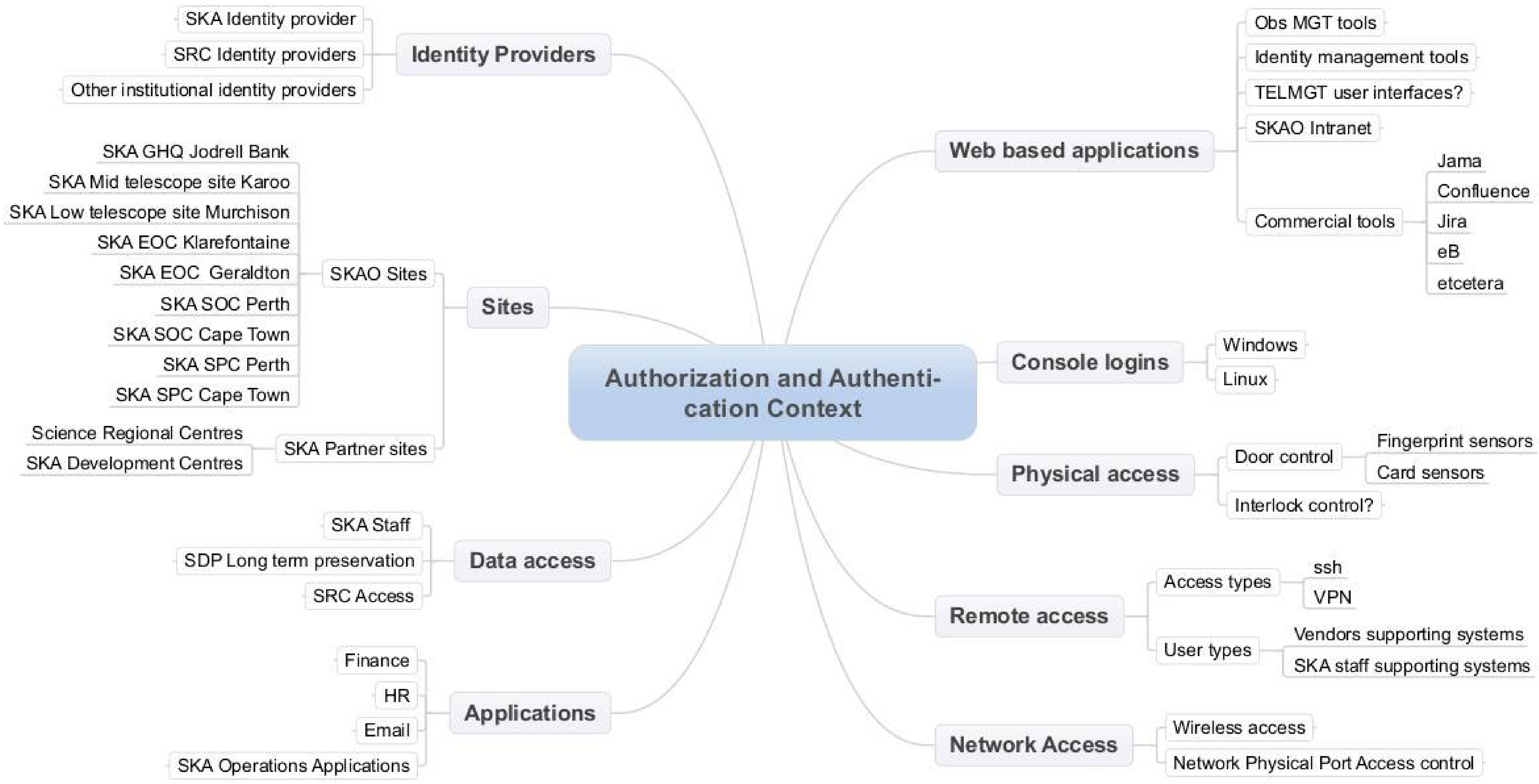
SKA
SQUARE KILOMETRE ARRAY






anzska
Square Kilometre Array • Australia • New Zealand
● Potential array station
SKA - AU
5,500km baseline

SKA A&A context



SKA A&A General Requirements

- Authentication service
  - available to all SKA elements
  - available off line
  - support the generation of user's credentials
  - provided of a management system interface
  - support the change of credentials (username/password)
  - allow cancellation of user
  - highly available (about 99.999%)
  - centralized management logical location
  - able to handle every kind of protocols (SAML, OpenID, OAuth, X509...)
  - Interoperable with a list of IdPs
  - Allow physical access
- Authorization service
  - available to all SKA elements
  - Compatible with various grouping systems
  - provided of a management system interface
  - able to handle different user’s roles, groups and privileges
  - shall follow the Policy statements
  - shall allow some group users to generate sub-groups and assign privileges to them
  - should be customized at each telescope site since some users like operators could be in principle operate in one location only
  - Interoperable within a federation with other grouping management systems
  - Interoperable with a list of CA
  - Allow access to granted people to restricted areas.

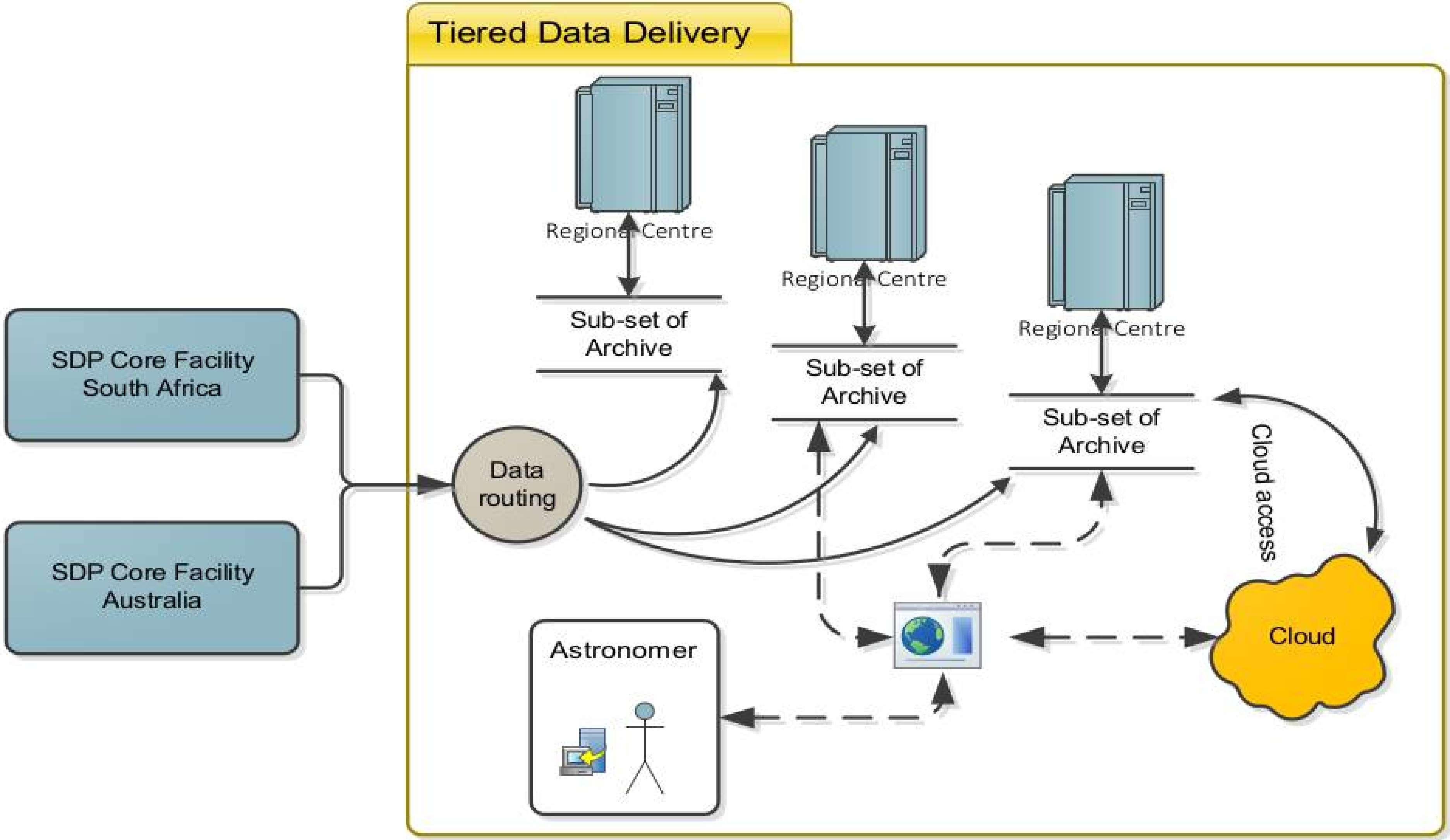
AuthN and AuthZ product

Purpose
The scope of the A&A is to define and implement all the functionalities necessary to identify a digital identity using self registration or federated recognition of users and grant access to specific services. The A&A technological possible solutions are various and mature but not all of them are interoperable. The possible issues are related to the interoperability of those systems.

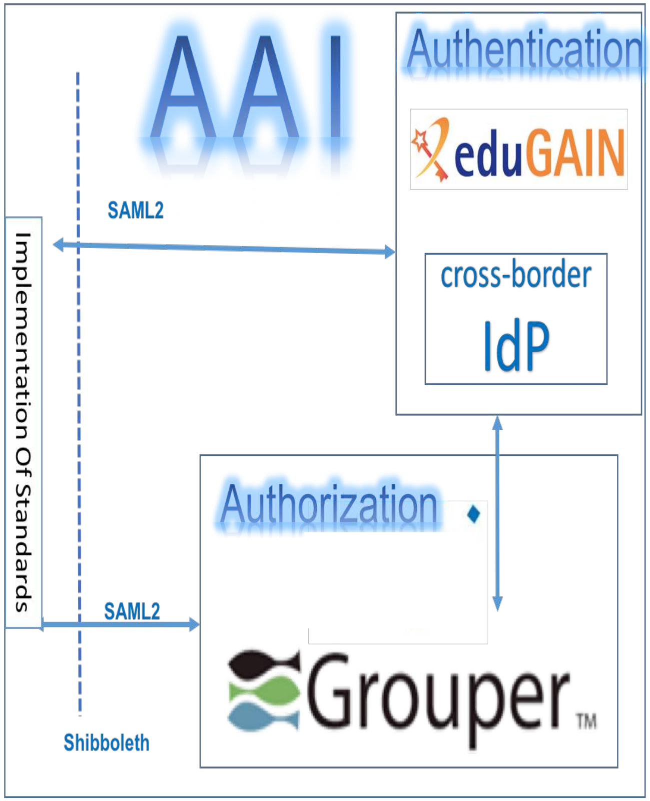
Requirements refer to a enterprise solution.

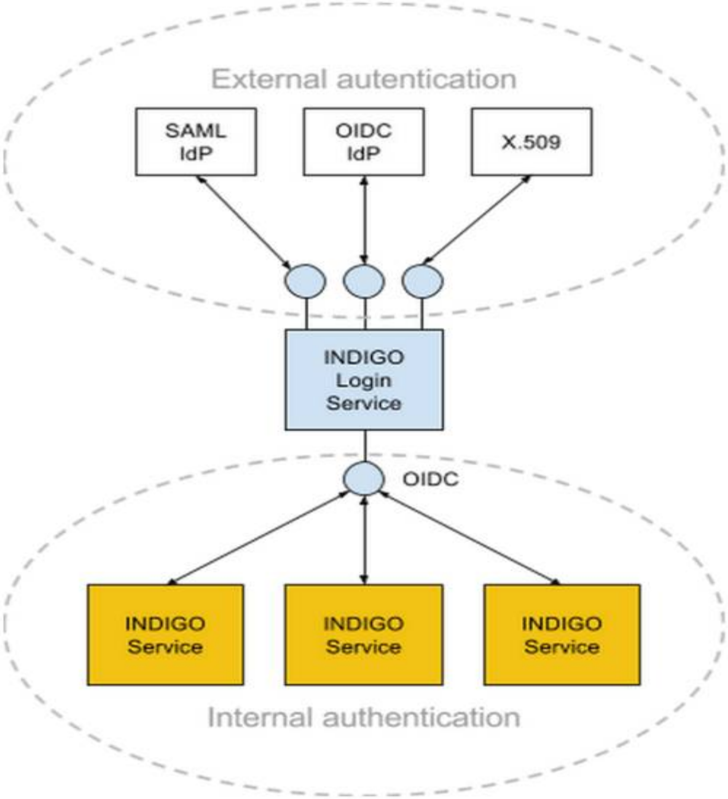
AENEAS H2020 project (approved) and SDP Delivery subsystem have to foreseen mechanisms to share data and authorizations.

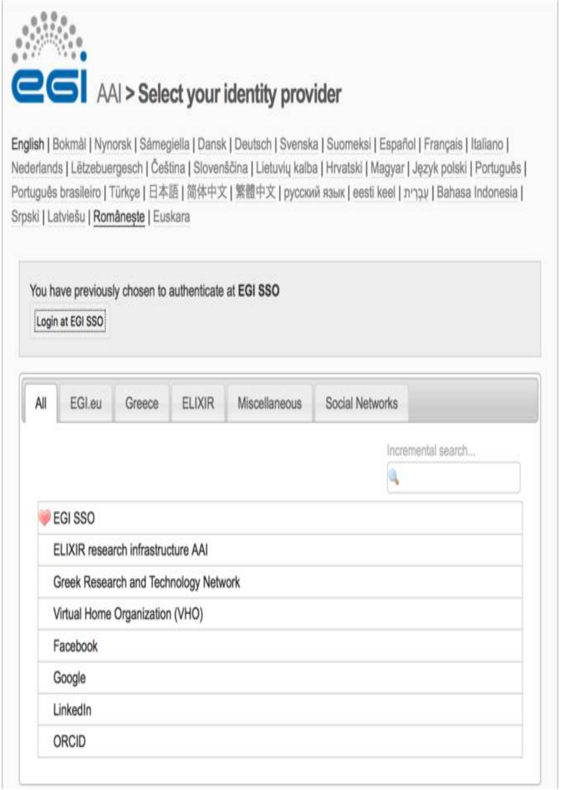
SKA and the SDC



AAA H2020 solutions







AAI > Select your identity provider

English | Bokmål | Nynorsk | Sámegiella | Dansk | Deutsch | Svenska | Suomeksi | Español | Français | Italiano | Nederlands | Lëtzebuergesch | Čeština | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 简体中文 | 繁體中文 | русский язык | eesti keel | עִבְרִית | Bahasa Indonesia | Srpski | Latviešu | Românește | Euskara

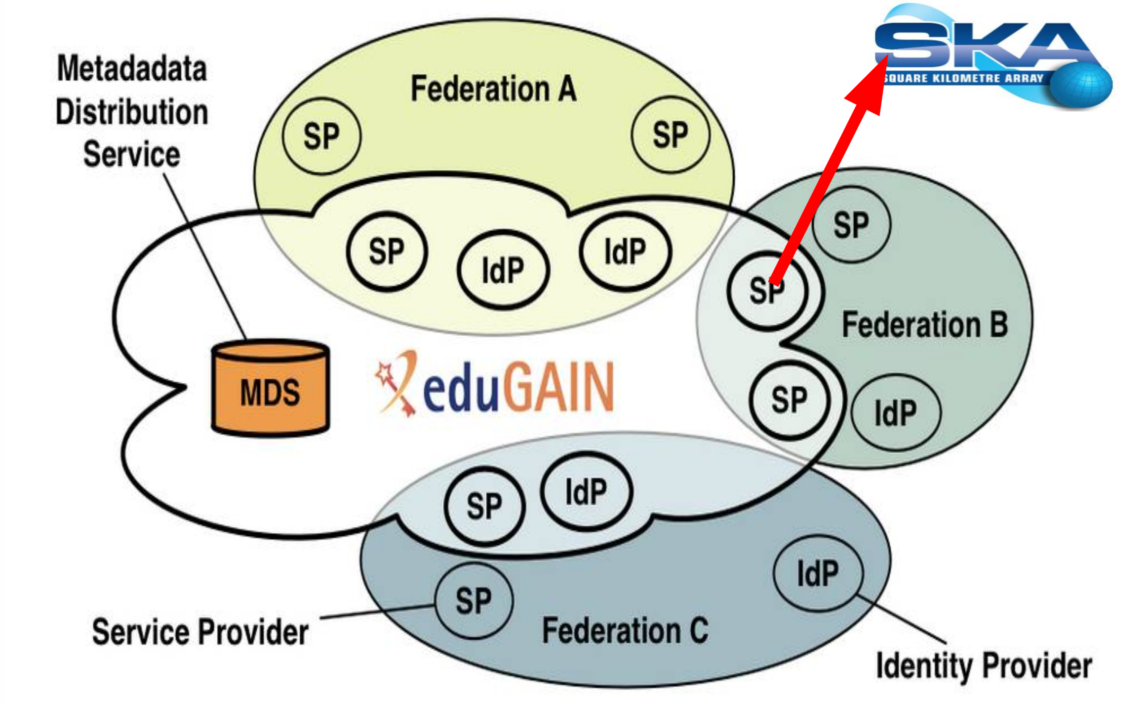
You have previously chosen to authenticate at **EGI SSO**

- EGI SSO
- ELIXIR research infrastructure AAI
- Greek Research and Technology Network
- Virtual Home Organization (VHO)
- Facebook
- Google
- LinkedIn
- ORCID

Asterics
Astronomy ESFRI & Research Infrastructure Cluster

INDIGO - DataCloud

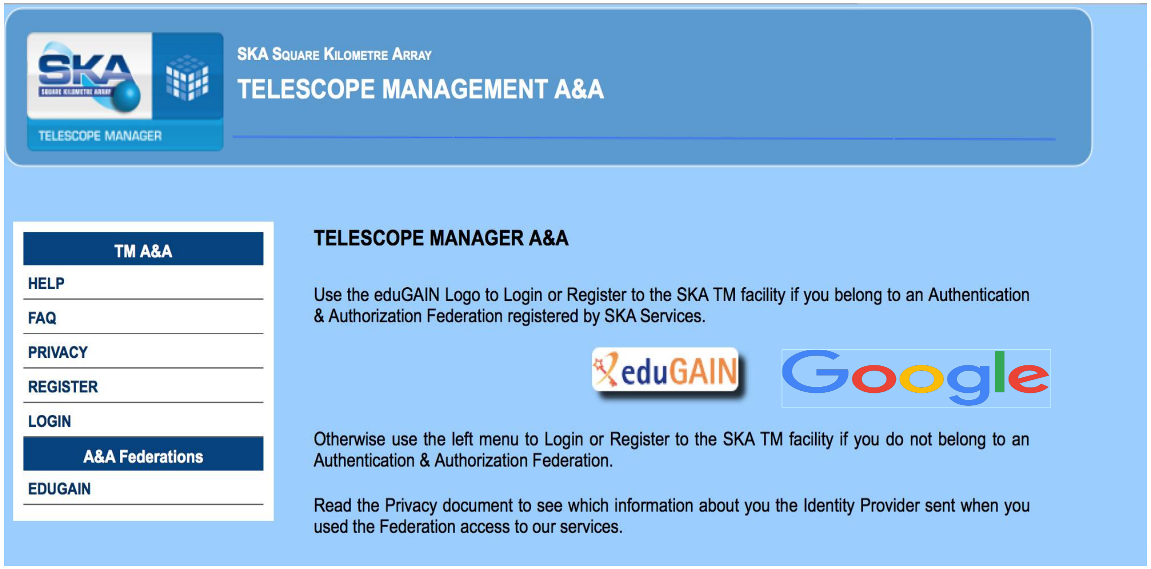
Current idea for Authentication



First step: implement a SERVICE provider for SKA means being able to authenticate identities already present in EduGAIN.

Second step: implement an identity provider for SKA in order to manage identities inside the SKA.

Third step: support other technologies for AIM (authentication interface management)



SKA Square Kilometre Array

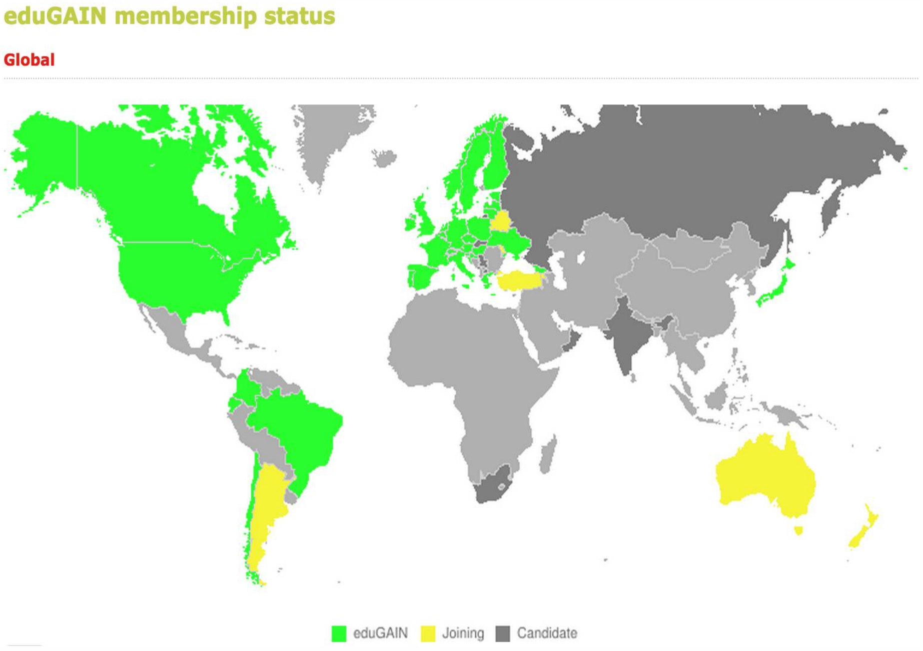
TELESCOPE MANAGEMENT A&A

TELESCOPE MANAGER A&A

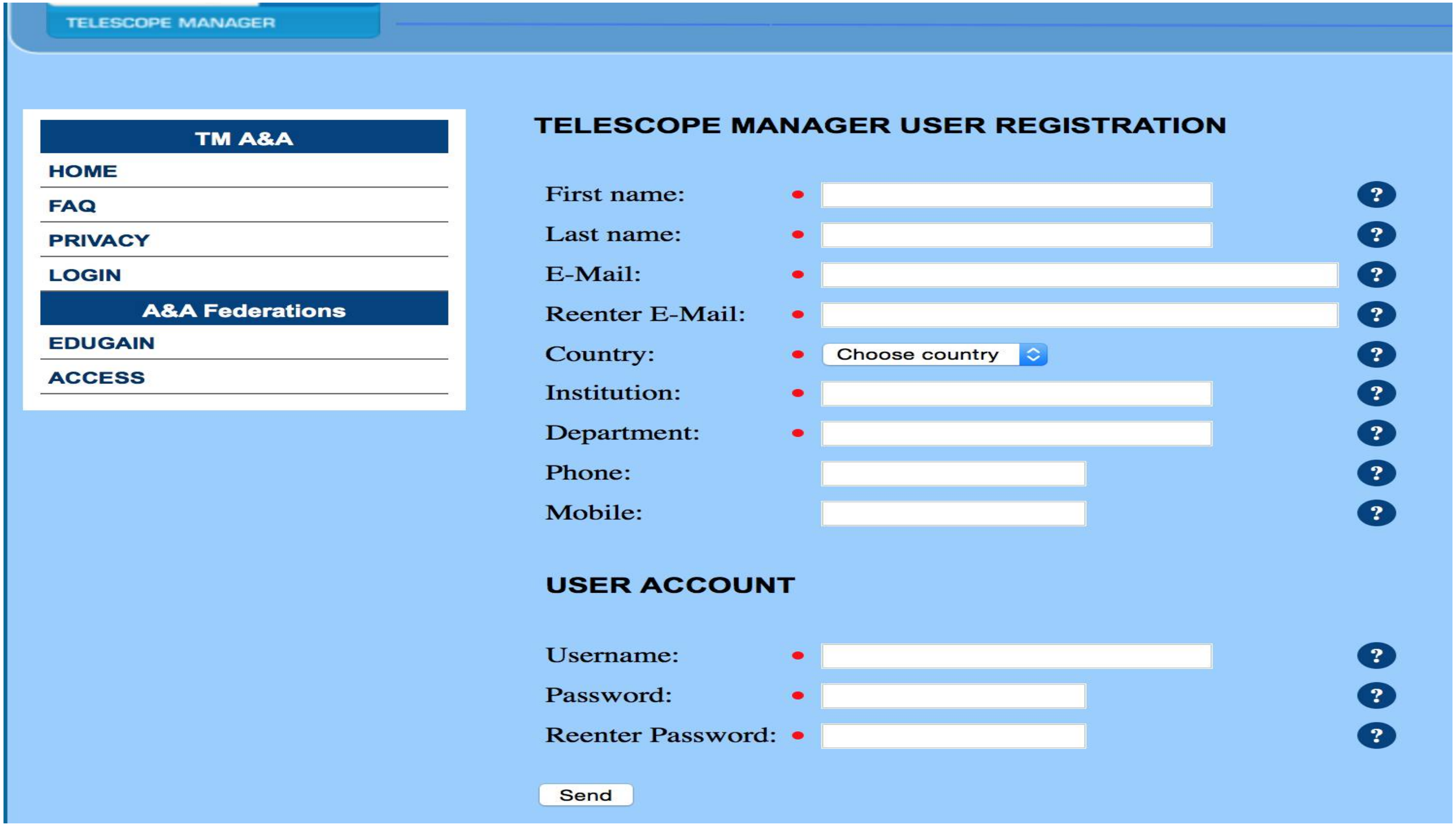
Use the eduGAIN Logo to Login or Register to the SKA TM facility if you belong to an Authentication & Authorization Federation registered by SKA Services.

Otherwise use the left menu to Login or Register to the SKA TM facility if you do not belong to an Authentication & Authorization Federation.

Read the Privacy document to see which information about you the Identity Provider sent when you used the Federation access to our services.



Self registration Authentication mechanism



TELESCOPE MANAGER USER REGISTRATION

First name: ●

Last name: ●

E-Mail: ●

Reenter E-Mail: ●

Country: ● Choose country

Institution: ●

Department: ●

Phone:

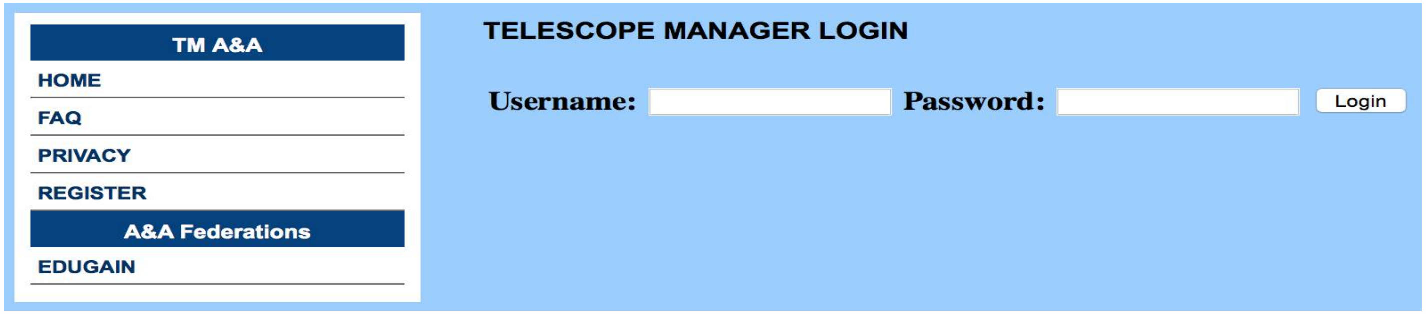
Mobile:

USER ACCOUNT

Username: ●

Password: ●

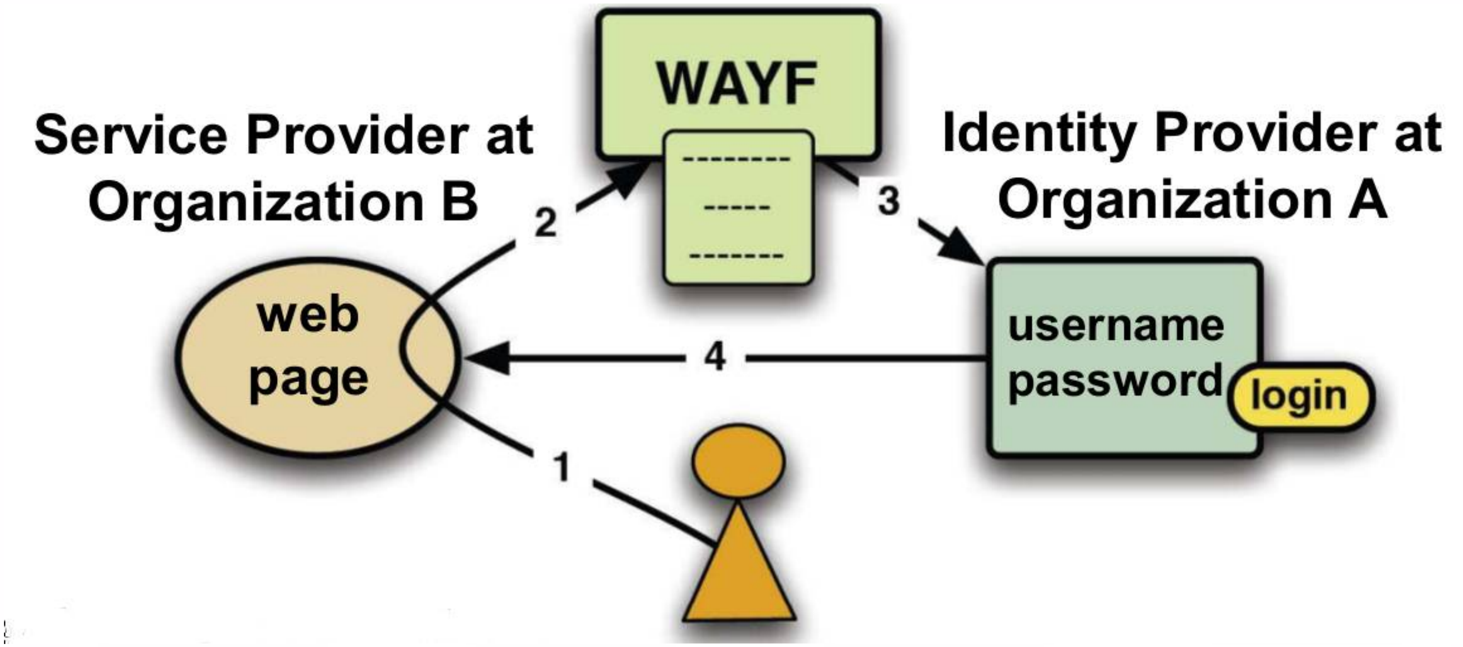
Reenter Password: ●

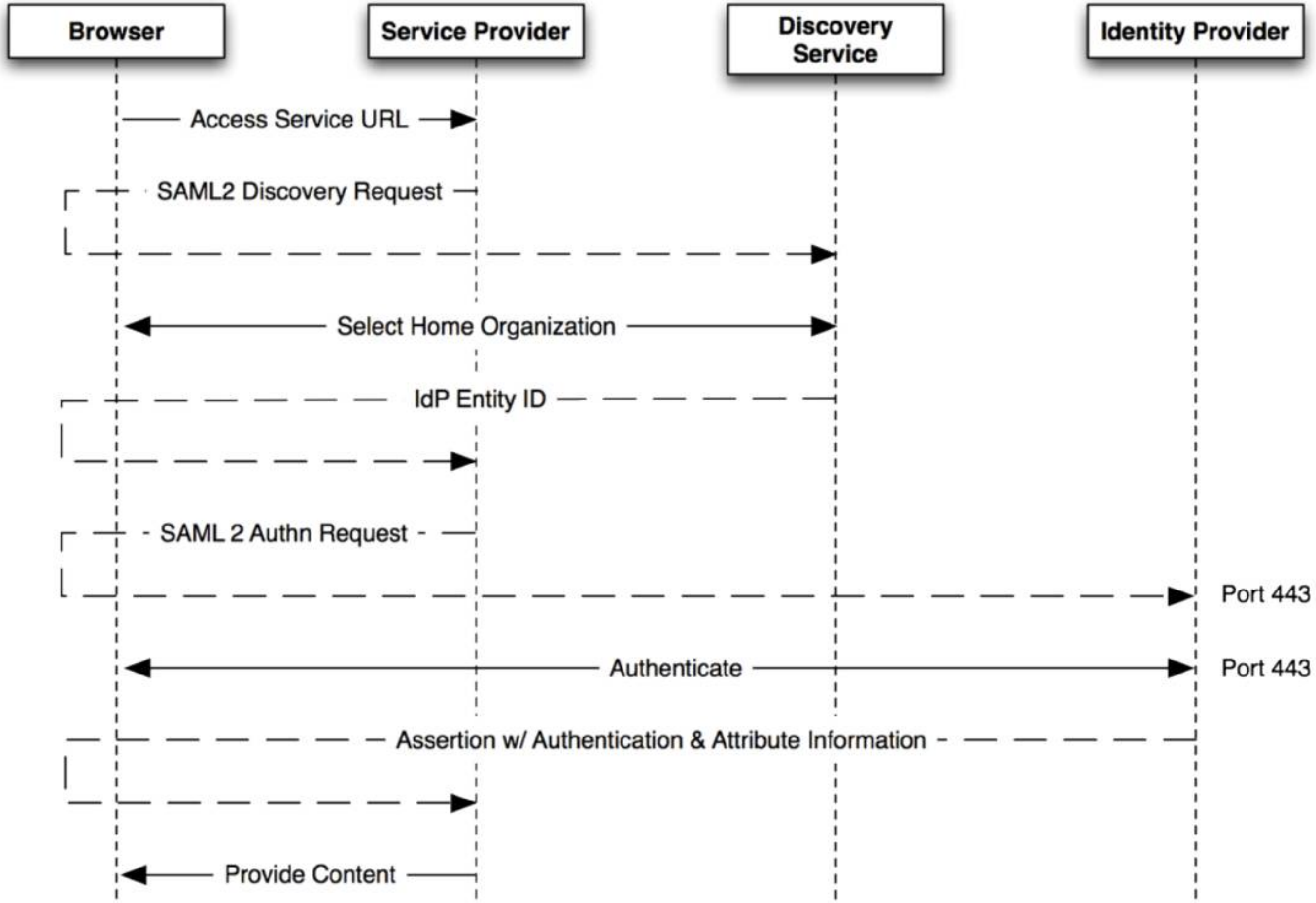


TELESCOPE MANAGER LOGIN

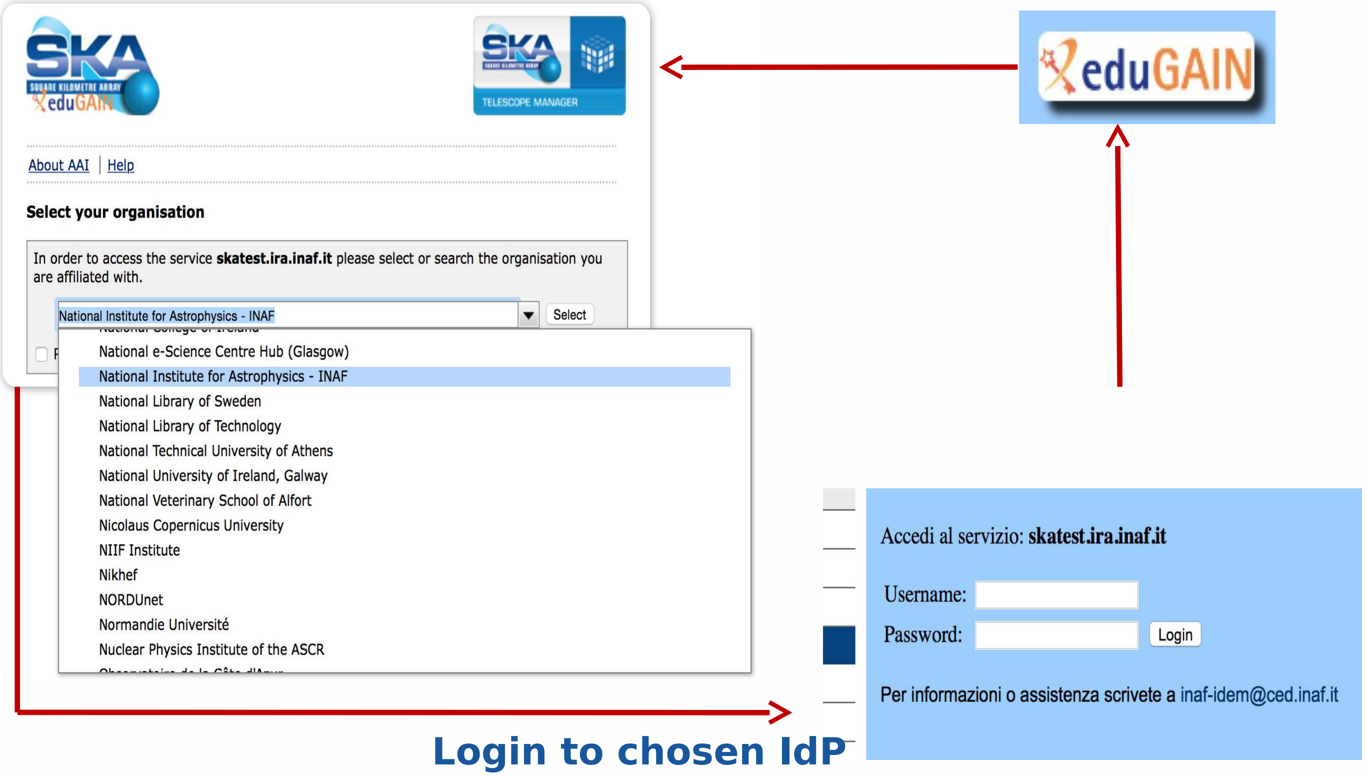
Username: Password:

Where Are You From (WAYF)


WAYF
Service Provider at Organization B
Identity Provider at Organization A
web page
username
password
login
1
2
3
4



WAYF and Federated Authentication mechanism



Select your organisation

In order to access the service **skatest.ira.inaf.it** please select or search the organisation you are affiliated with.

National Institute for Astrophysics - INAF ▼ Select

- National College of Ireland
- National e-Science Centre Hub (Glasgow)
- National Institute for Astrophysics - INAF
- National Library of Sweden
- National Library of Technology
- National Technical University of Athens
- National University of Ireland, Galway
- National Veterinary School of Alfort
- Nicolaus Copernicus University
- NIIF Institute
- Nikhef
- NORDUnet
- Normandie Université
- Nuclear Physics Institute of the ASCR
- Observatoire de la Côte d'Azur

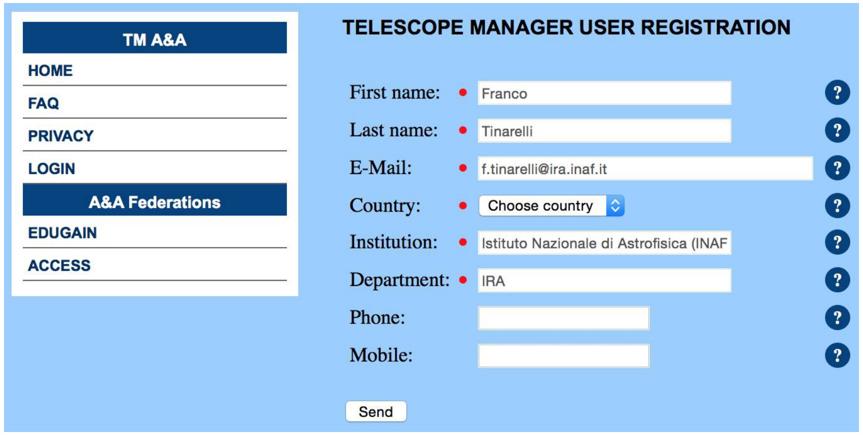
Accedi al servizio: **skatest.ira.inaf.it**

Username:

Password: Login

Per informazioni o assistenza scrivete a inaf-idem@ced.inaf.it

Login to chosen IdP

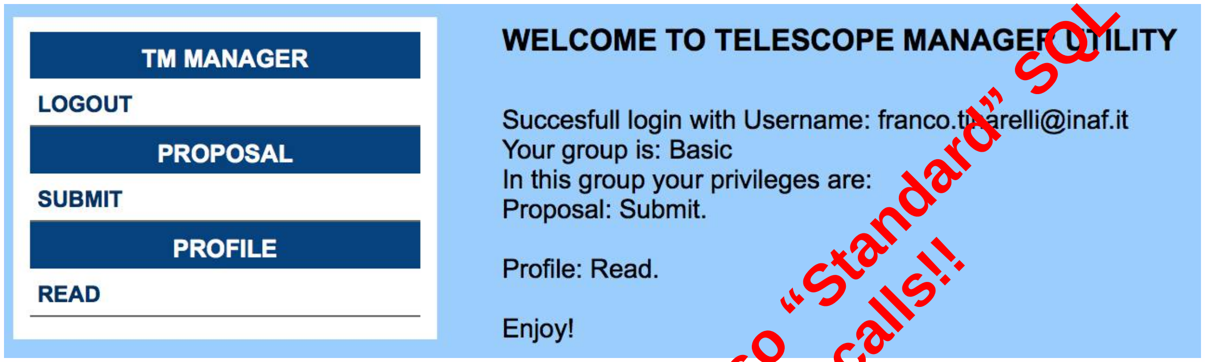


TELESCOPE MANAGER USER REGISTRATION

First name: •	Franco
Last name: •	Tinarelli
E-Mail: •	f.tinarelli@ira.inaf.it
Country: •	Choose country
Institution: •	Istituto Nazionale di Astrofisica (INAF
Department: •	IRA
Phone:	
Mobile:	

Send

SKA Authorization: existing and future plans

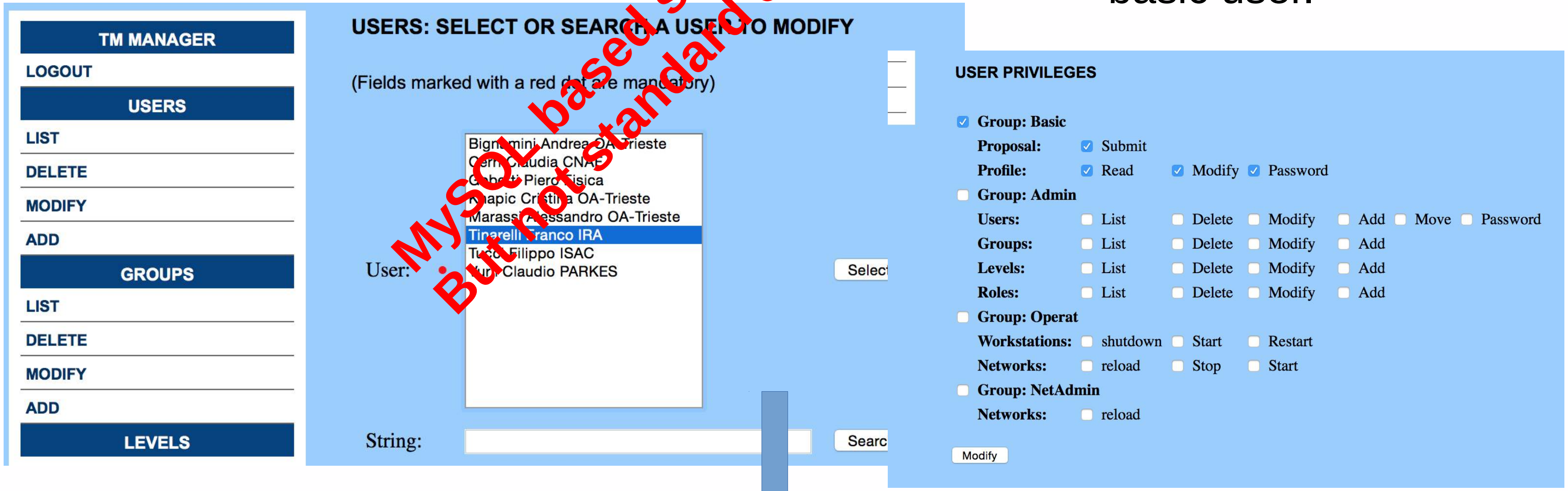


WELCOME TO TELESCOPE MANAGER UTILITY

Succesfull login with Username: franco.tinarelli@inaf.it
Your group is: Basic
In this group your privileges are:
Proposal: Submit.

Profile: Read.

Enjoy!



USERS: SELECT OR SEARCH A USER TO MODIFY

(Fields marked with a red dot are mandatory)

User: ●
Bignamini Andrea OA-Trieste
Cerri Claudia CNAF
Gabotti Piero Fisica
Knapic Cristina OA-Trieste
Marassi Alessandro OA-Trieste
Tinarelli Franco IRA
Tucci Filippo ISAC
Yuri Claudio PARKES

String:

USER PRIVILEGES

☑ **Group: Basic**

Proposal:	☑ Submit					
Profile:	☑ Read	☑ Modify	☑ Password			

☐ **Group: Admin**

Users:	☐ List	☐ Delete	☐ Modify	☐ Add	☐ Move	☐ Password
Groups:	☐ List	☐ Delete	☐ Modify	☐ Add		
Levels:	☐ List	☐ Delete	☐ Modify	☐ Add		
Roles:	☐ List	☐ Delete	☐ Modify	☐ Add		

☐ **Group: Operat**

Workstations:	☐ shutdown	☐ Start	☐ Restart
Networks:	☐ reload	☐ Stop	☐ Start

☐ **Group: NetAdmin**

Networks:	☐ reload

MySQL based so “Standard” SQL

But not standard calls!!

First step: basic authorization.

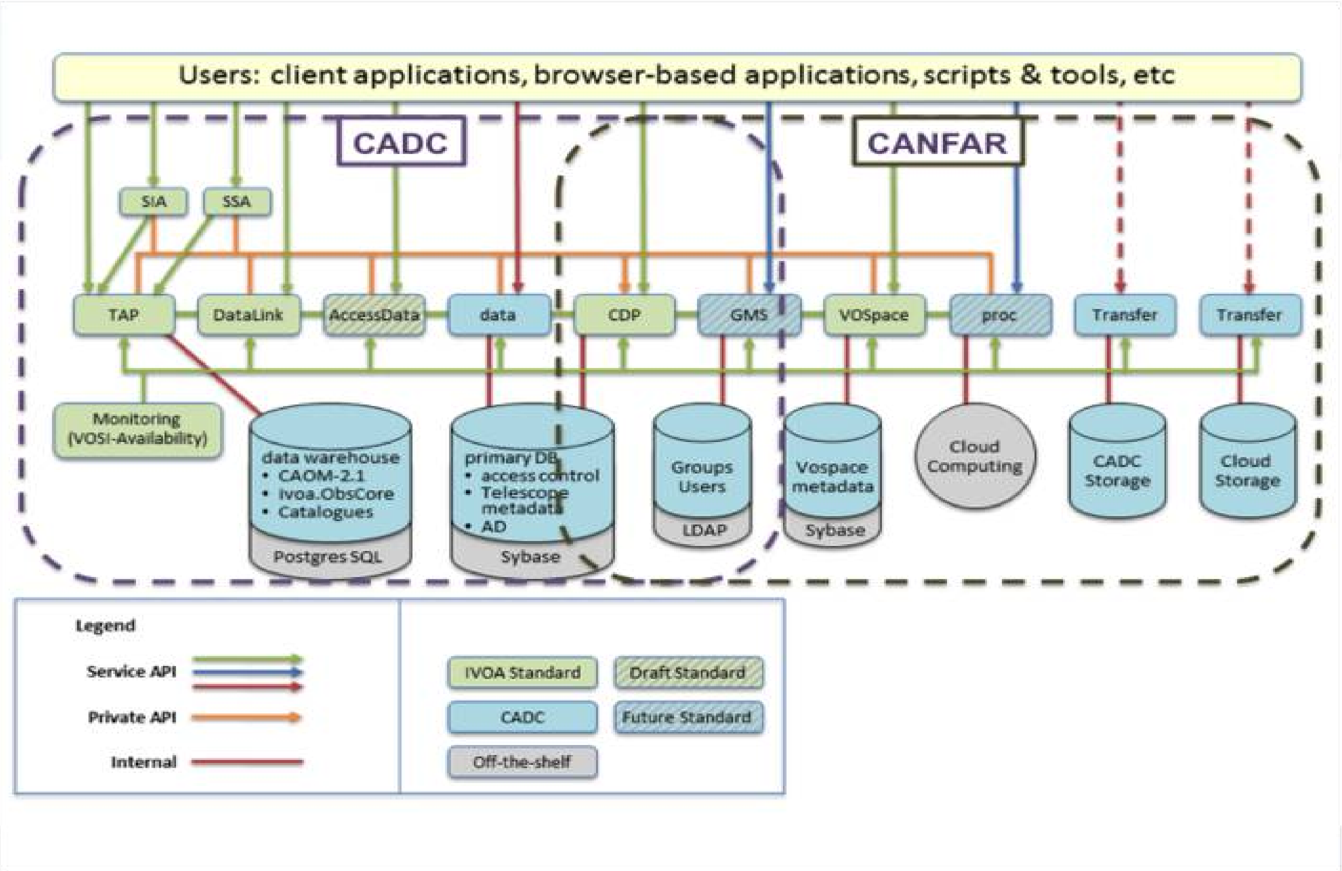
Second step: SKA administrator manage group affiliation and roles/privileges for each non basic user.

Suggestion: use standards as much as possible interoperable with the VO! → GMS/Grouper

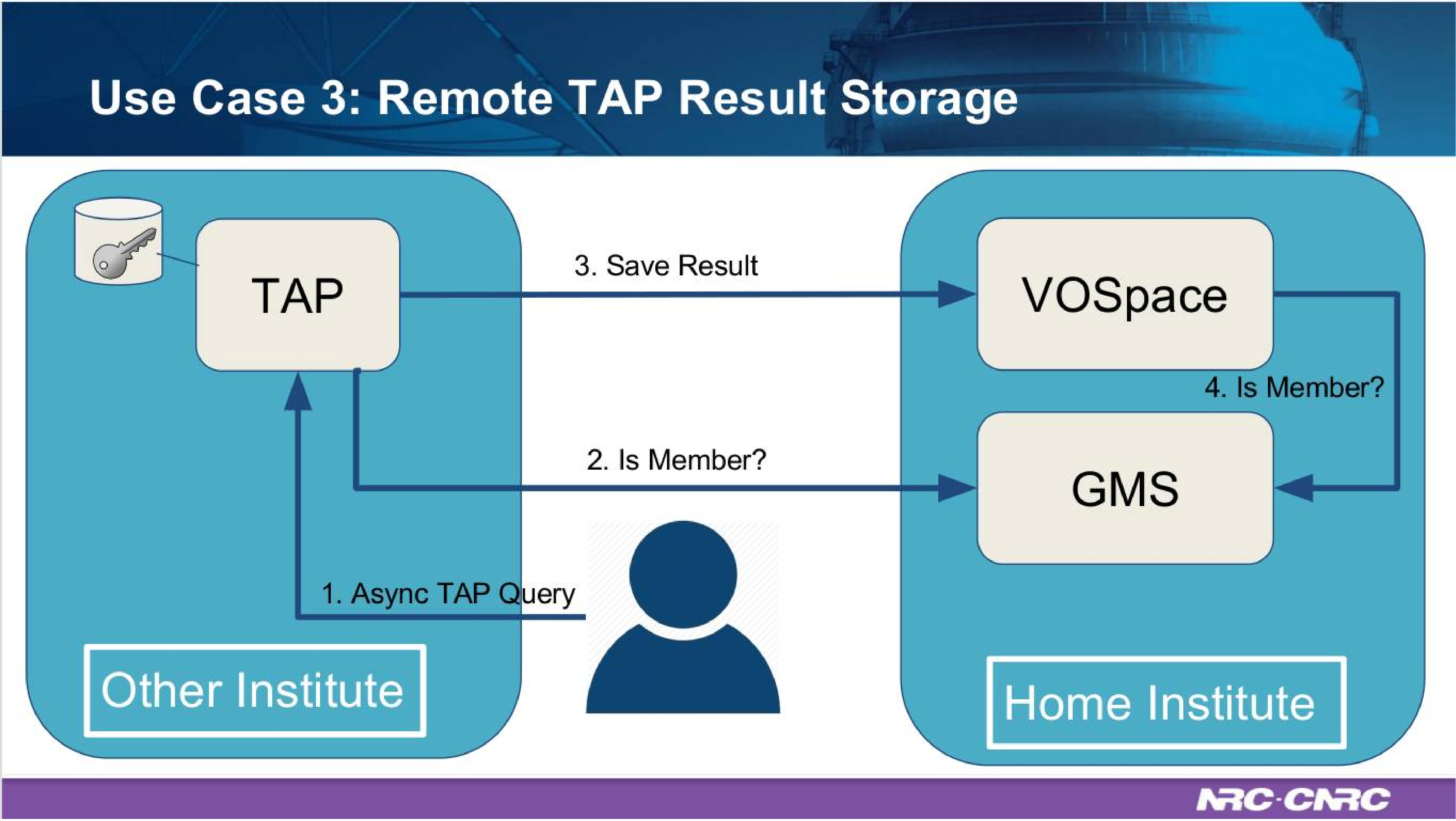
GMS solution

The service integrates and complements other access control related IVOA standards such as single-sign-on (SSO) using X.509 proxy certificates and the Credential Delegation Protocol (CDP).
– Groups are identified with unique URIs Ex:
ivo://cadc.nrc.ca/GEMINI-PI-GS-2011-Q-11
– Group Members identified with their X.509 Distinguished Name Ex:
CN=Adrian Damian,OU=hia.nrc.ca,O=Grid,C=CA

GMS hosts are interoperable and independent of each other. Each service maintains its own group membership list.



GMS federation mechanism



Use Case 3: Remote TAP Result Storage

Courtesy of B. Major

Conclusions

- Hard work to do to interoperate with multiple infrastructures
- Strength collaboration with VO compliant facilities (CADC,...)
- New perspective for enterprise solutions
- Thanks to our OATS colleagues for good hints and collaboration...

But for first........

Special thanks to Franco Tinarelli for the huge work done and useful collaboration.

Thank you for your attention!