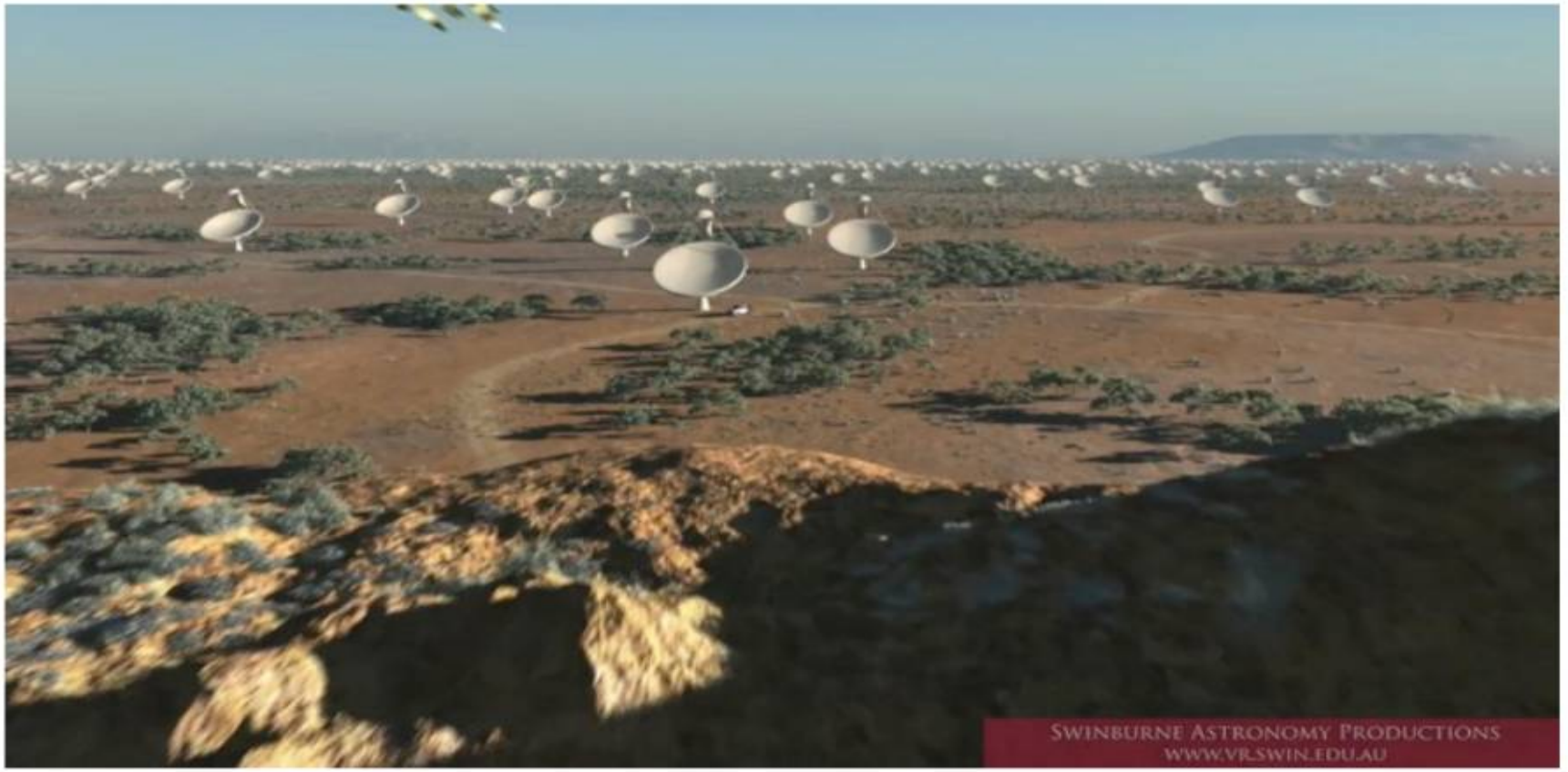
AAA @ SKA

Cristina Knapic

SKA

SQUARE KILOMETRE ARRAY

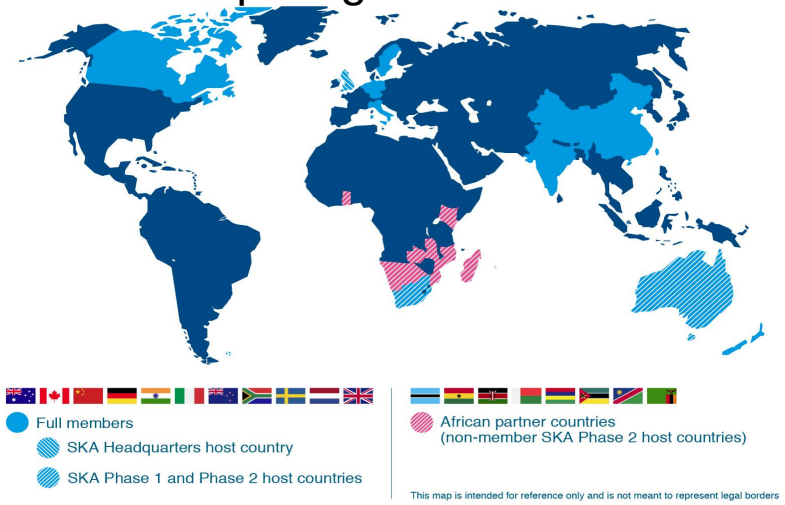


- 2020 era radio telescope
- Very large collecting area (km^2)
- Very large field of view
- Wide frequency range (70MHz - 25 GHz)
- Large physical extent (3000+ km)

- 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

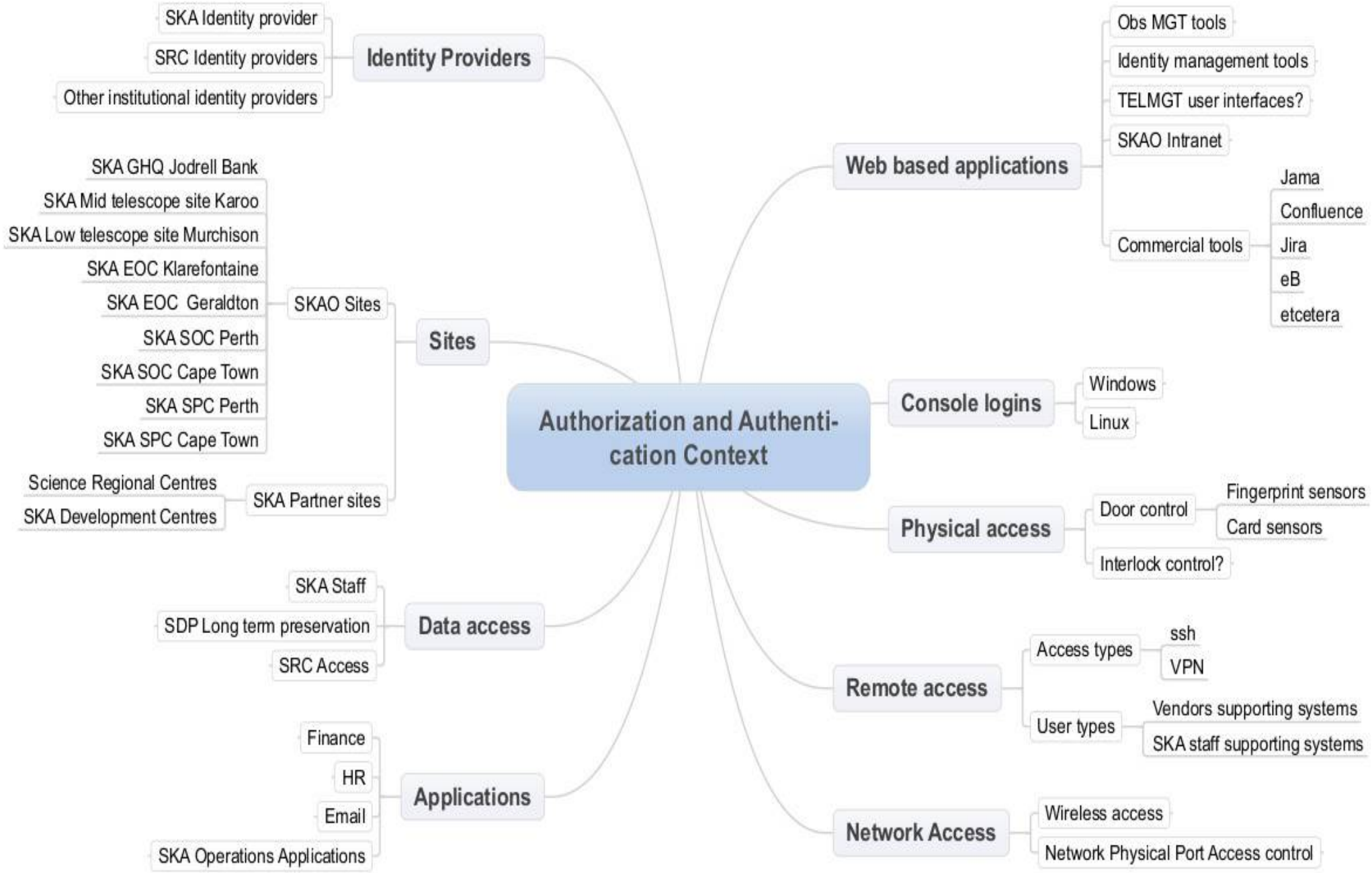
SKA Locations

Participating countries



SKA
SQUARE KILOMETRE ARRAY

SKA AAA context



SKA AAA 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

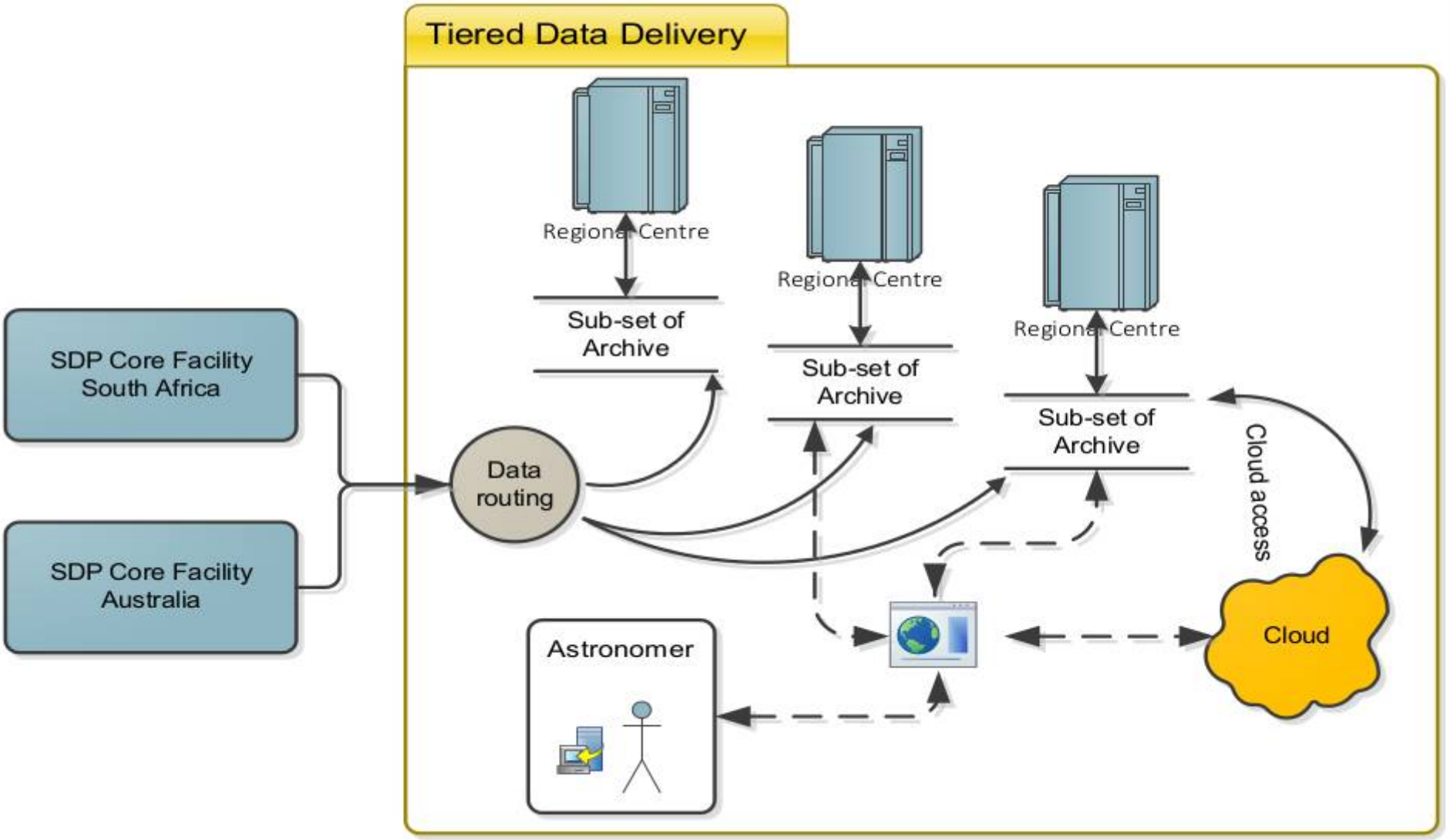
Purpose

The scope of the AAA 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 AAA 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.

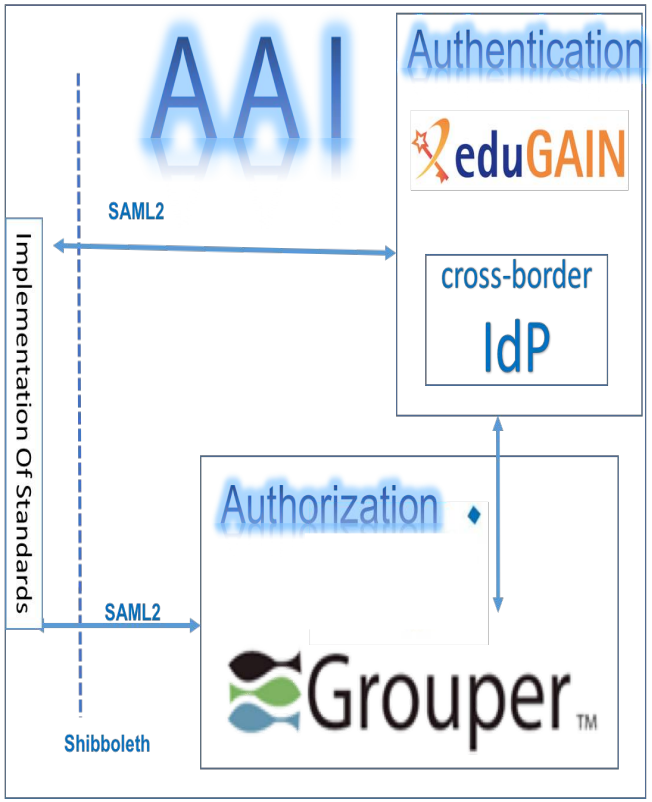
Requirements refer to a enterprise solution.

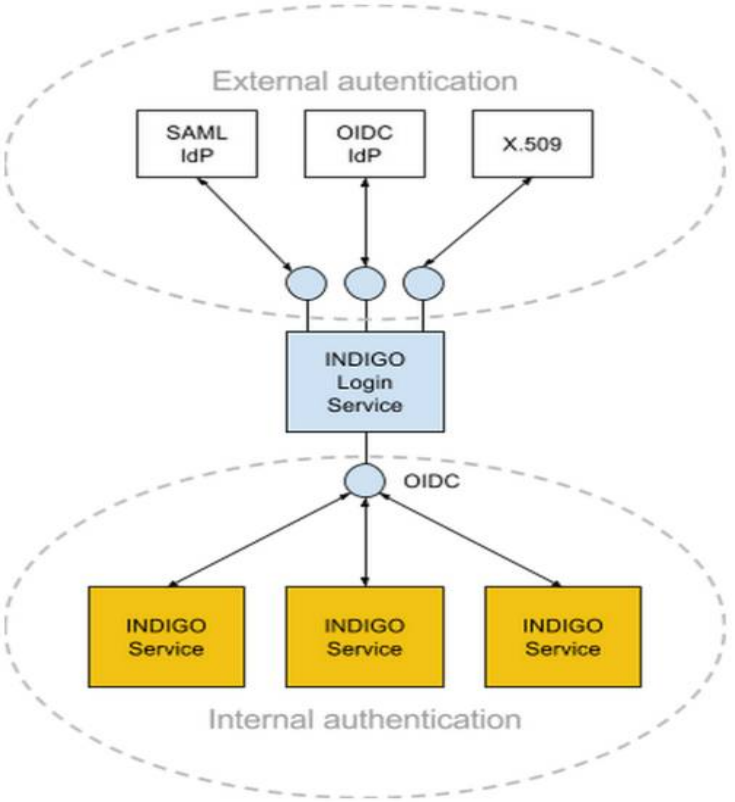
AENEAS H2020 project (approved) and SDP Delivery subsystem have to foreseen mechanisms to share data and authorizations.

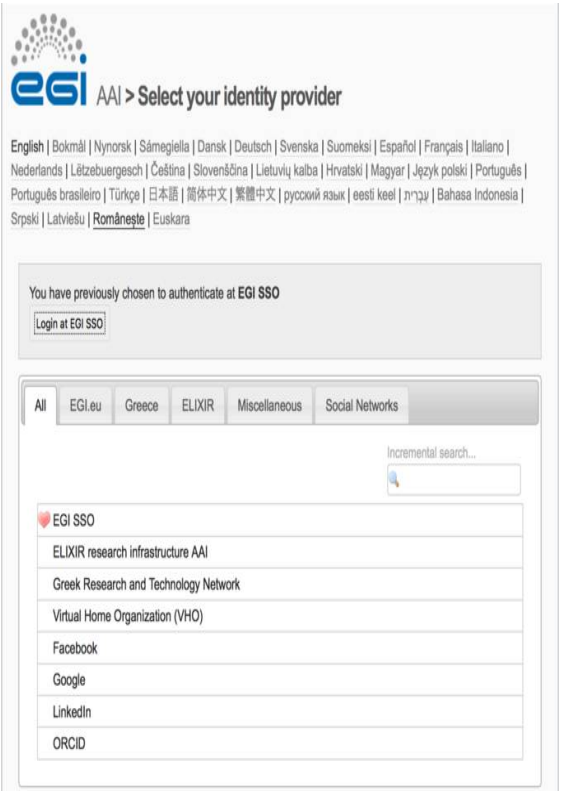
SKA and the SDC



AAA H2020 solutions





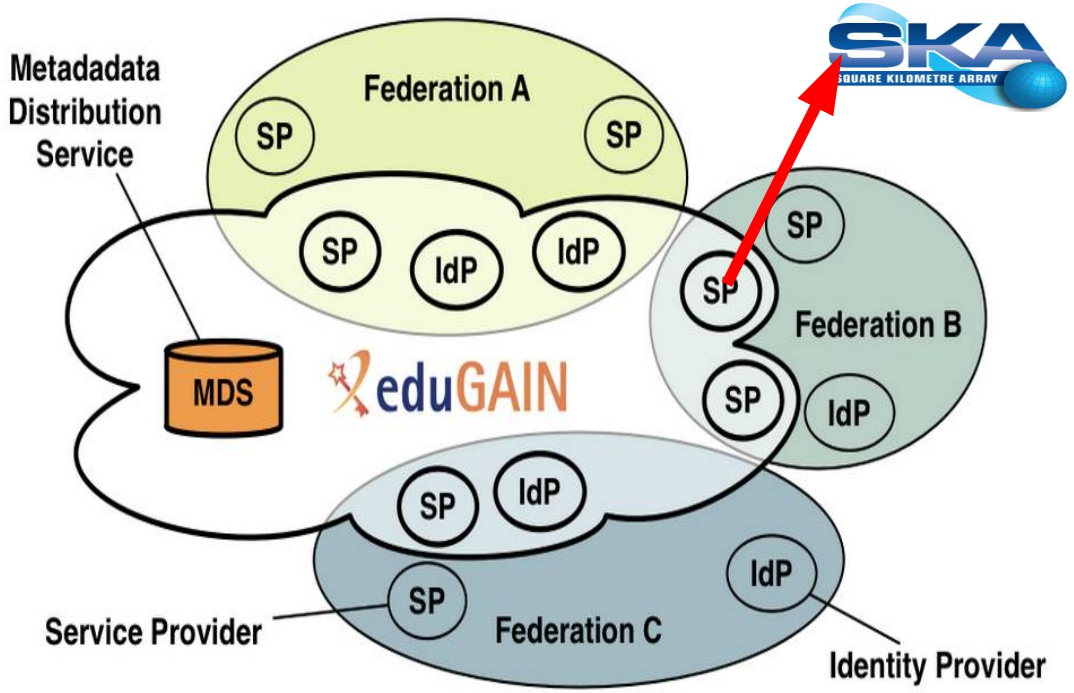


Asterics
Astronomy ESFRI & Research Infrastructure Cluster

INDIGO - DataCloud

EGI

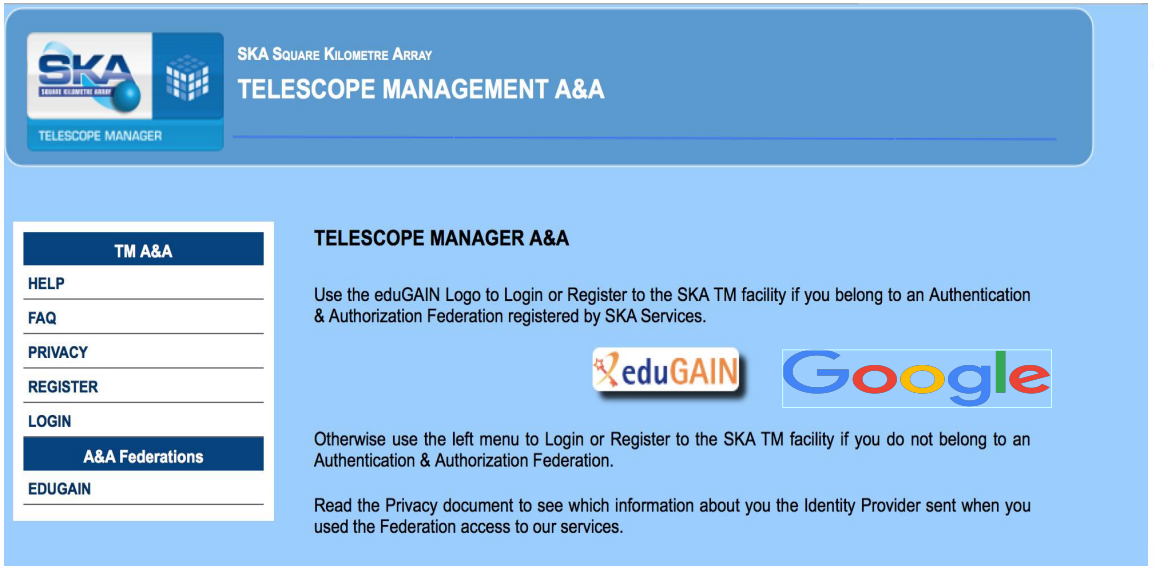
Current idea for Authentication

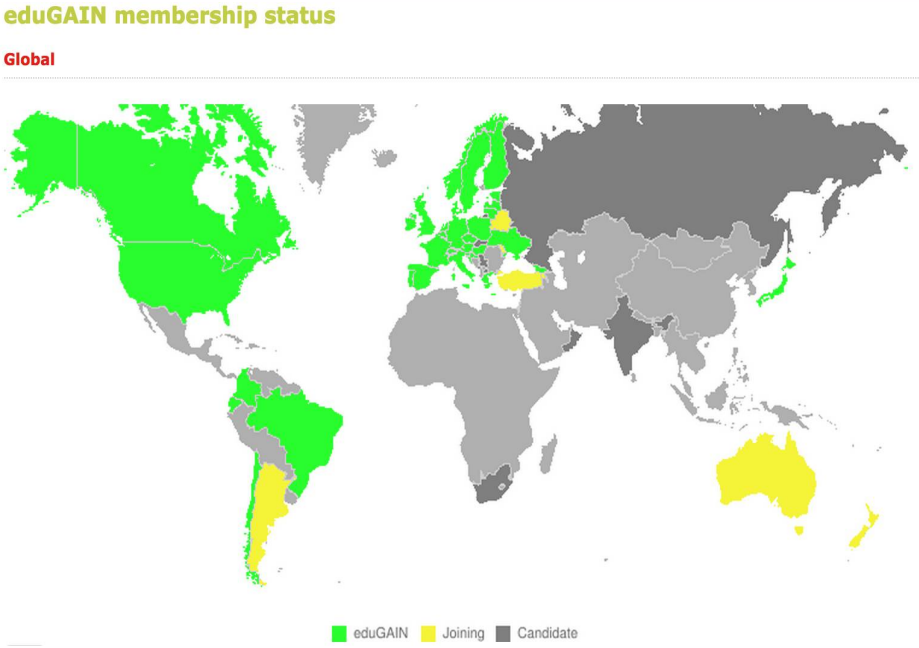


First step: implement a SERVICE provider for SKA means being able to authenticate identities already present in EduGAIN.

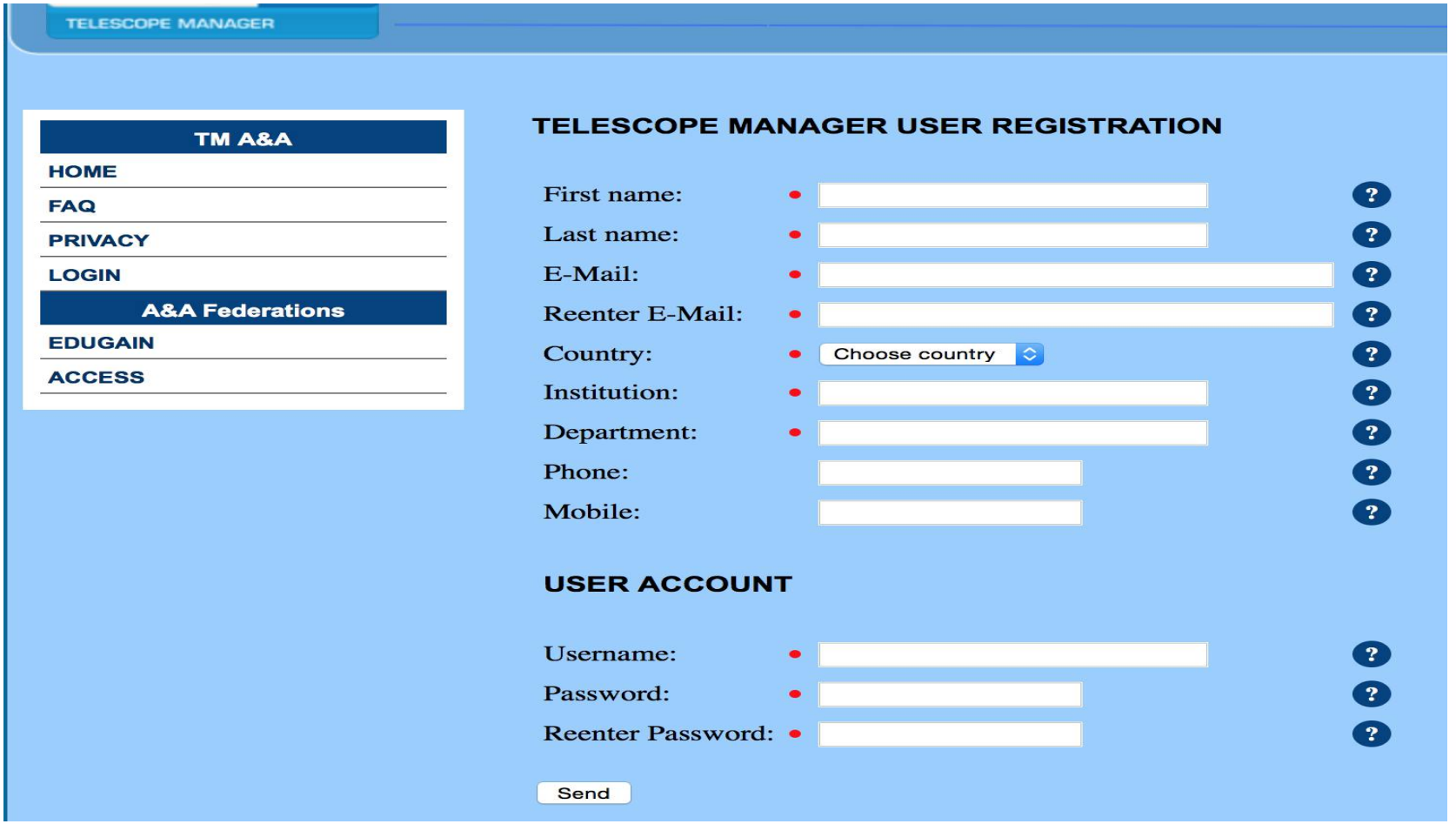
Second step: implement an identity provider for SKA in order to manage identities inside the SKA.

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

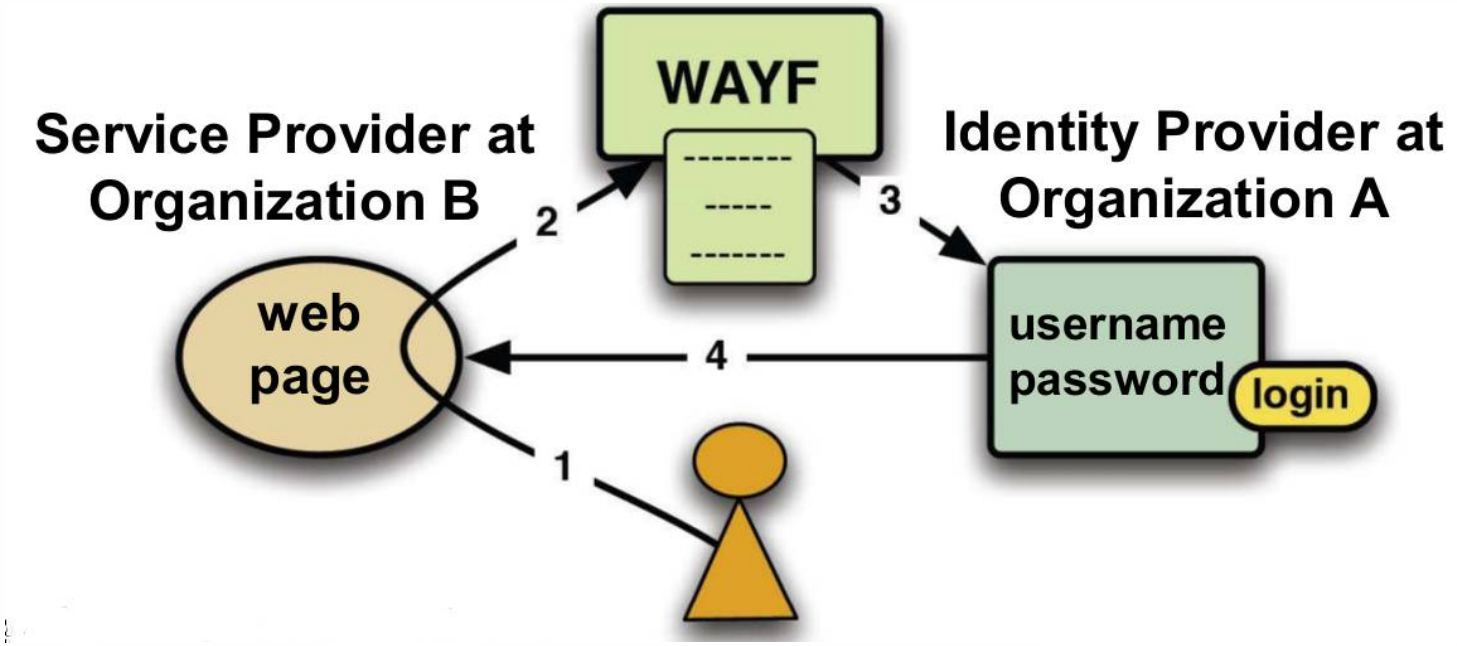


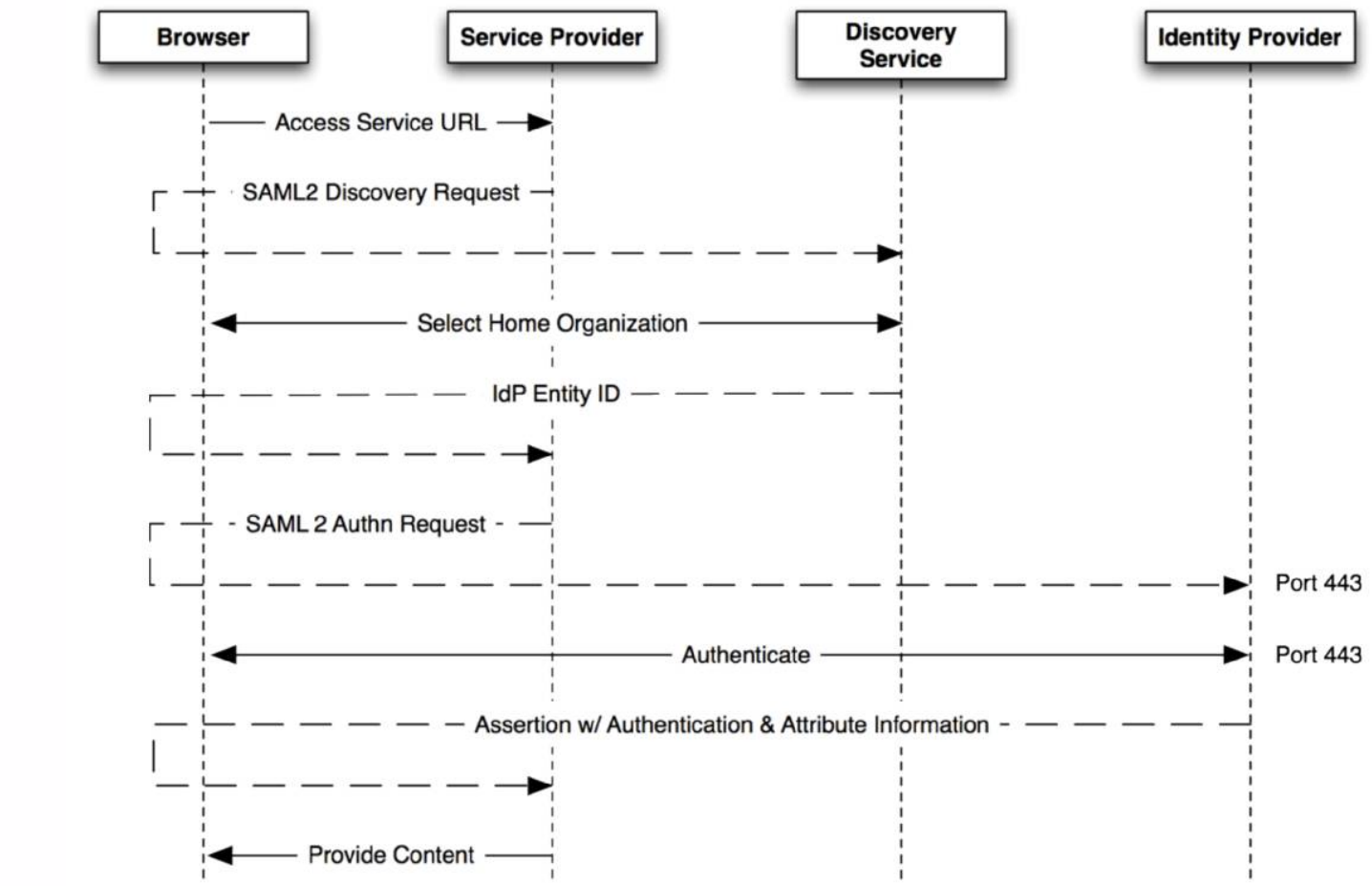


Self registration Authentication mechanism

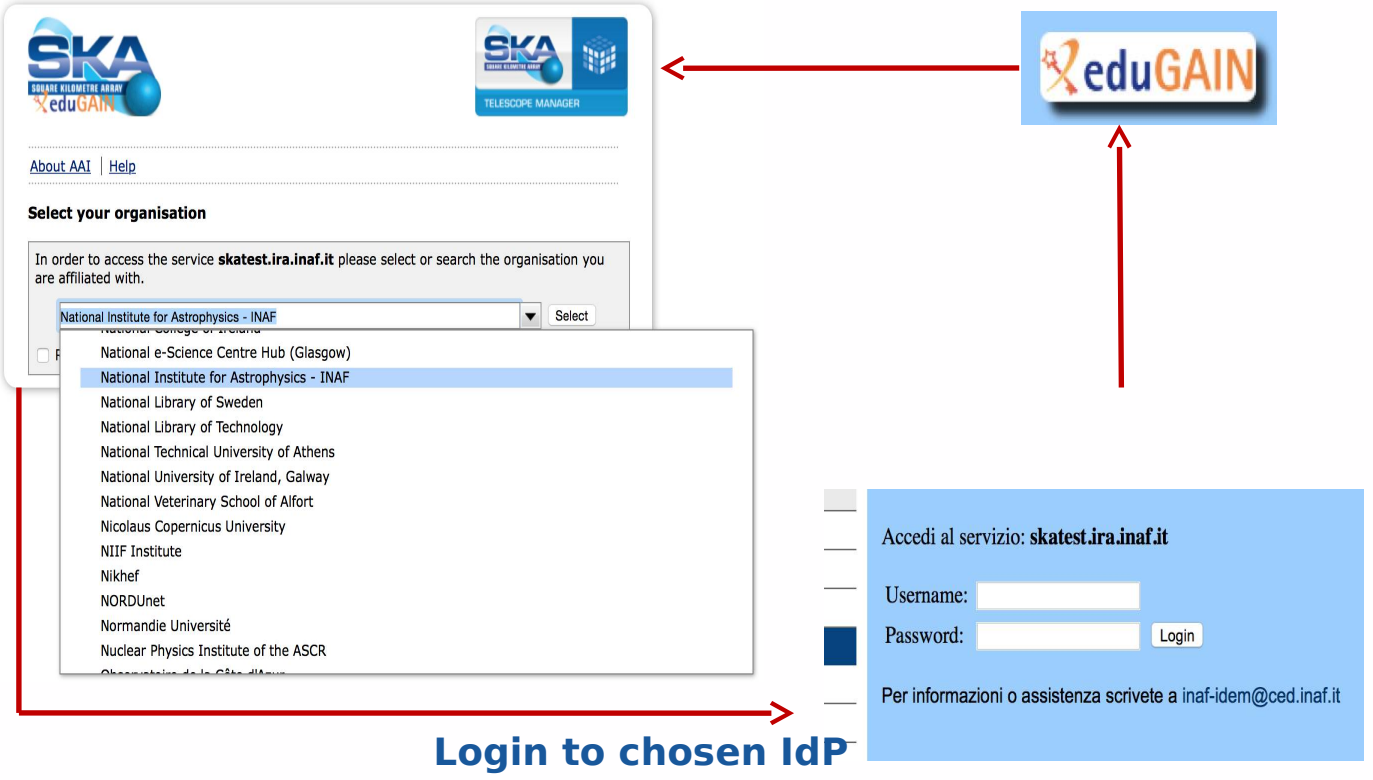


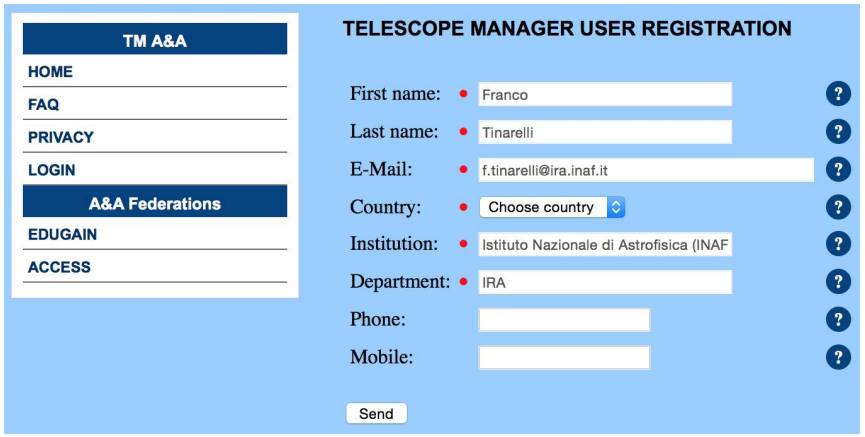
Where Are You From (WAYF)



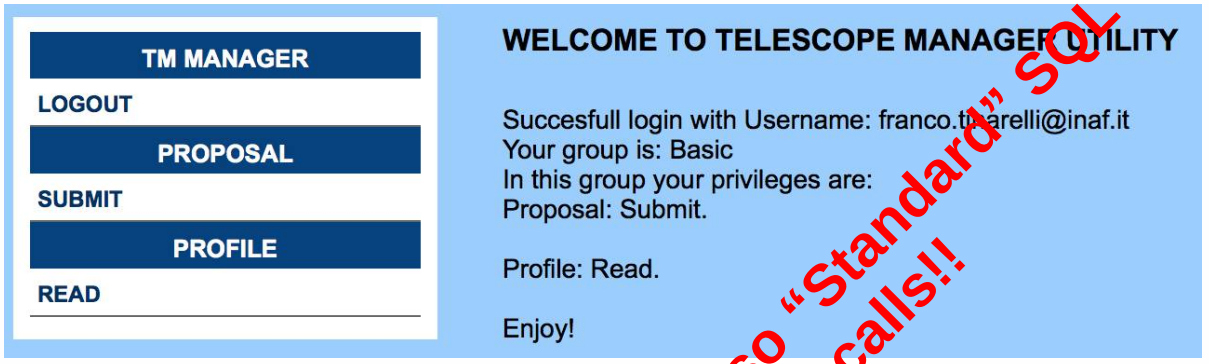


WAYF and Federated Authentication mechanism





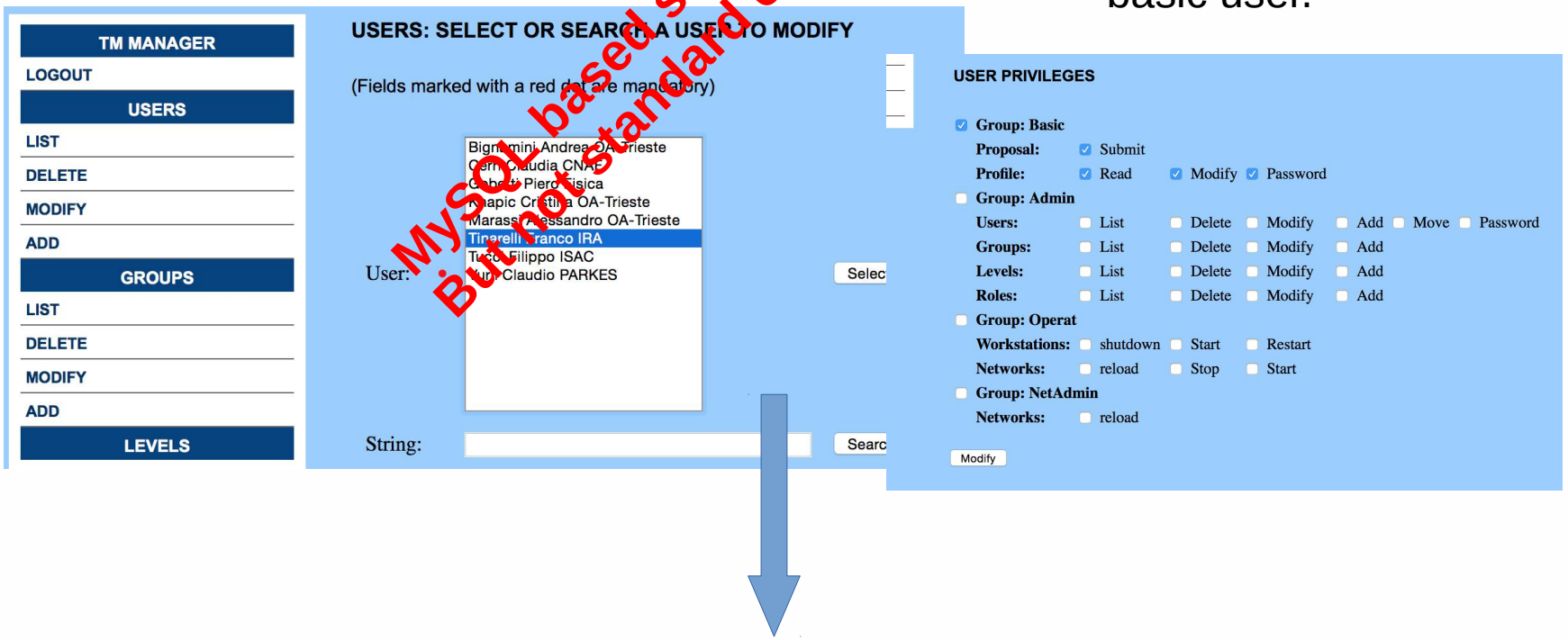
SKA Authorization: existing and future plans



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 within the VO! → **GMS/Grouper**

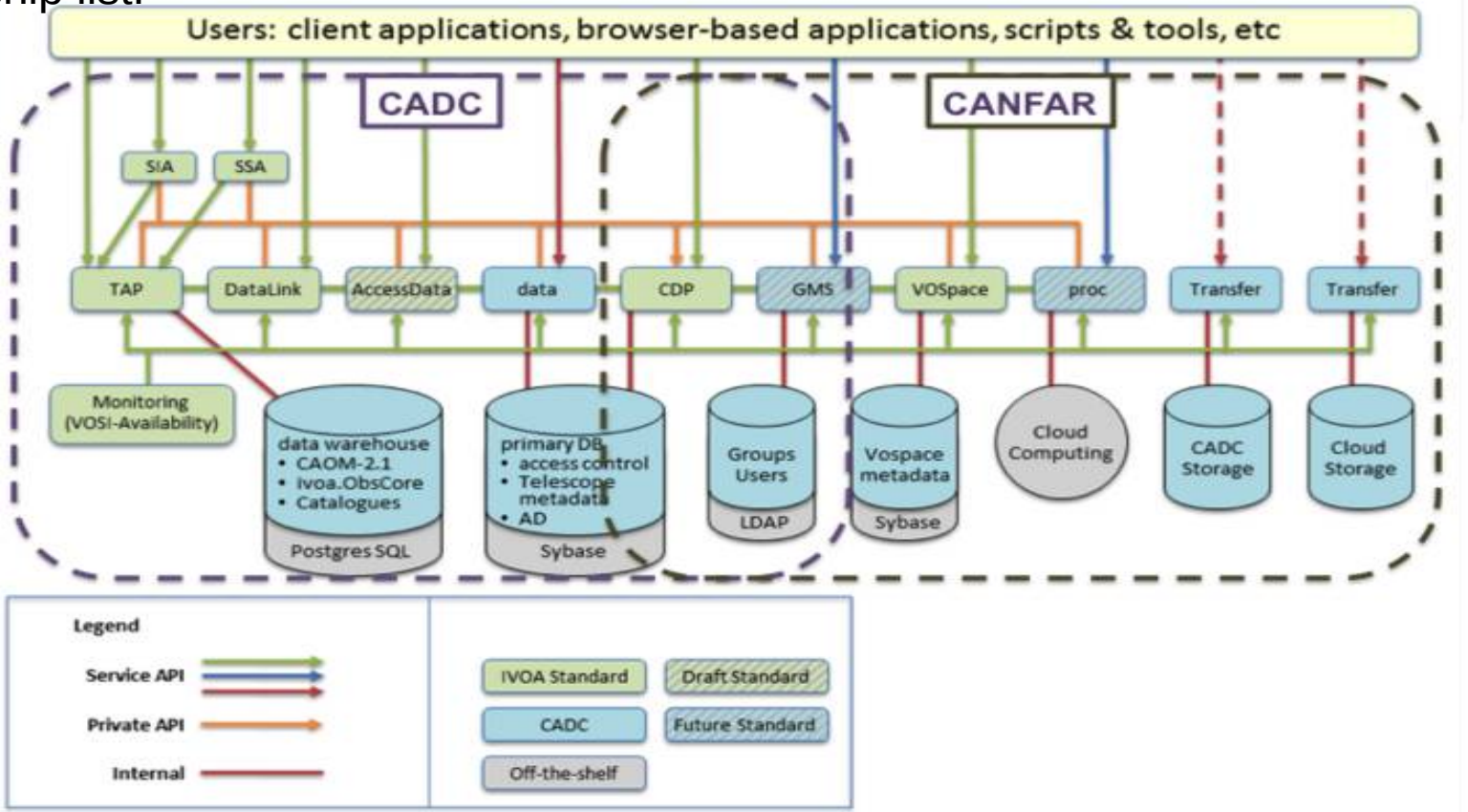
GMS solution

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**).

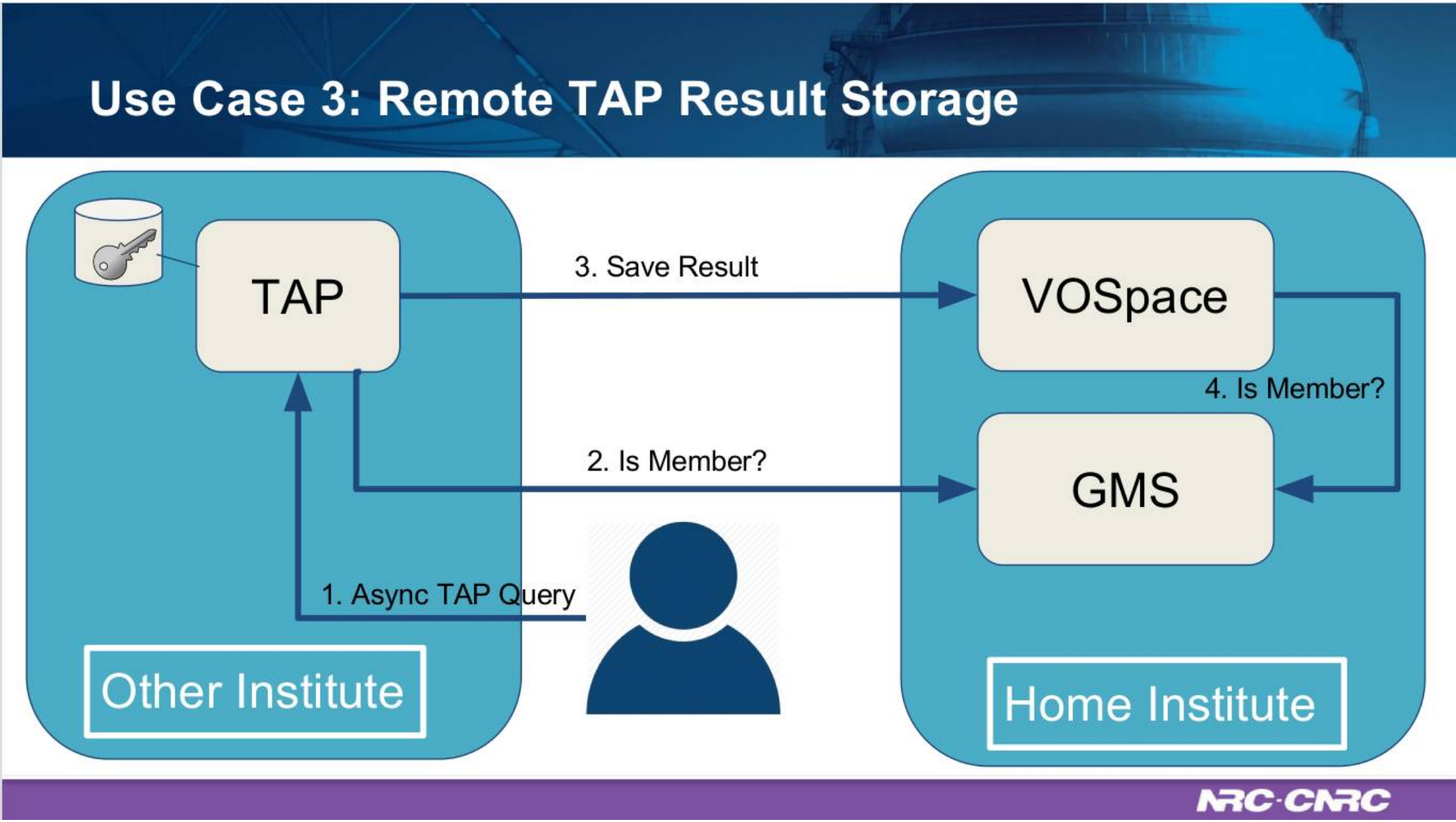
– Groups are identified with unique URIs Ex:
ivo://cadc.nrc.ca/GEMINI-PI-GS-2011-Q-11

– 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



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!