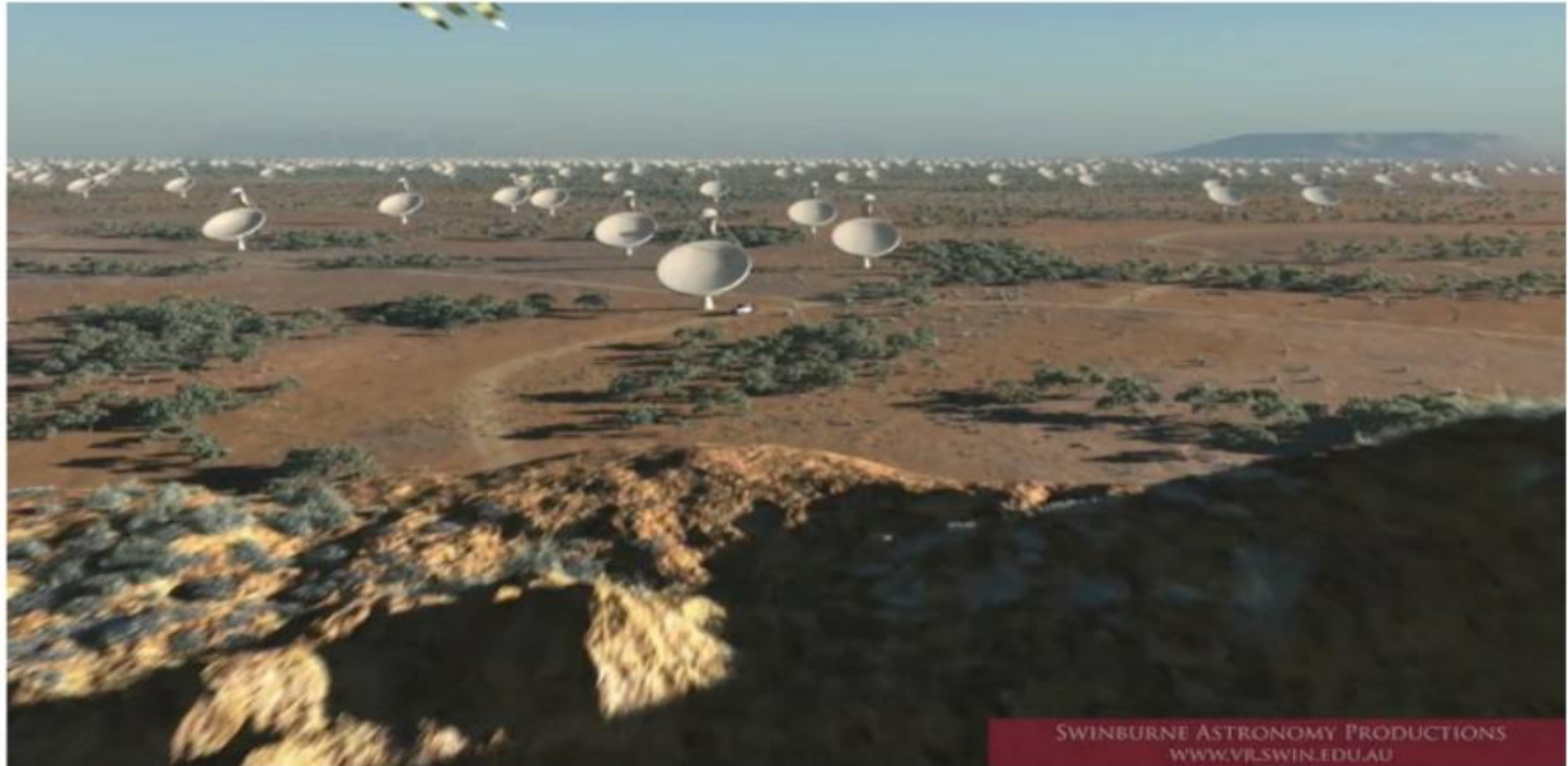


A night sky with the Milky Way galaxy and several large radio telescope dishes in a field. The dishes are illuminated from below, and the sky is dark with stars and the galaxy's light. The text "AAA @ SKA" is overlaid in the center, and "Cristina Knapic" is written in a cursive font below it.

AAA @ SKA

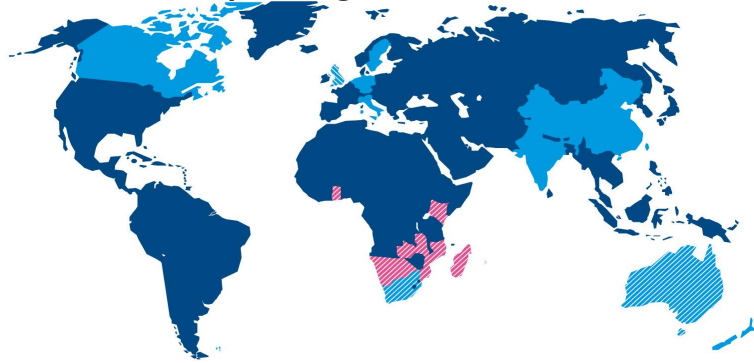
Cristina Knapic



- 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



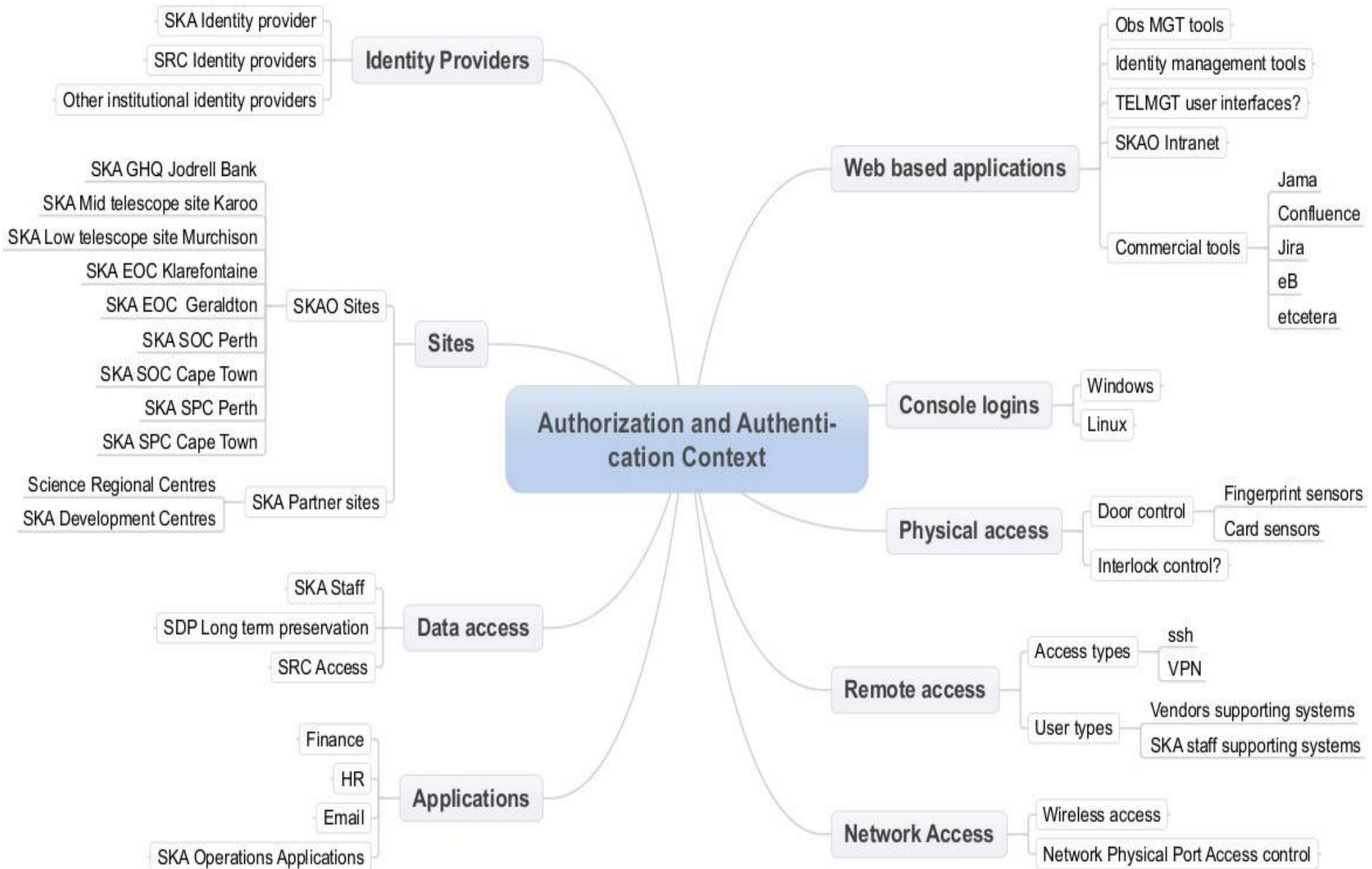
- Full members
- SKA Headquarters host country
- SKA Phase 1 and Phase 2 host countries
- African partner countries (non-member SKA Phase 2 host countries)

- 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 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

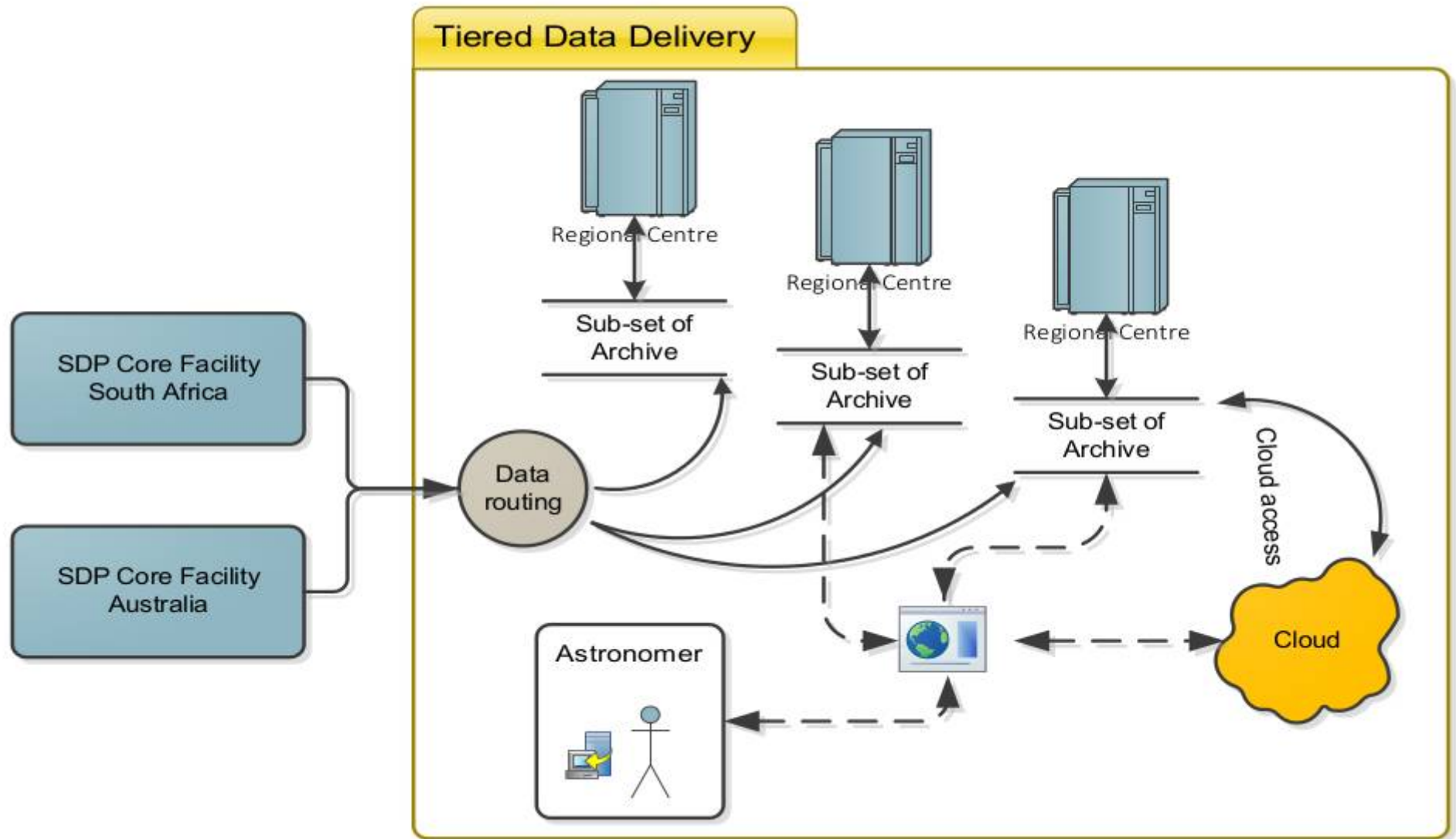
Purpose

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.

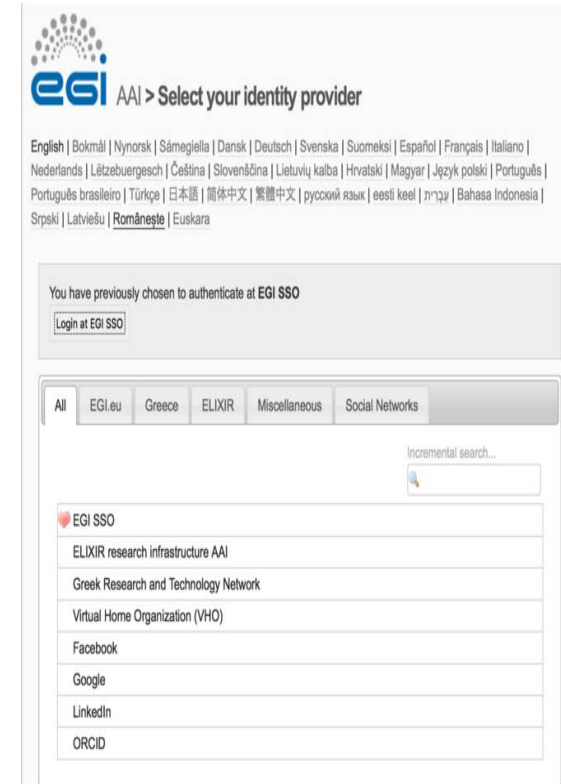
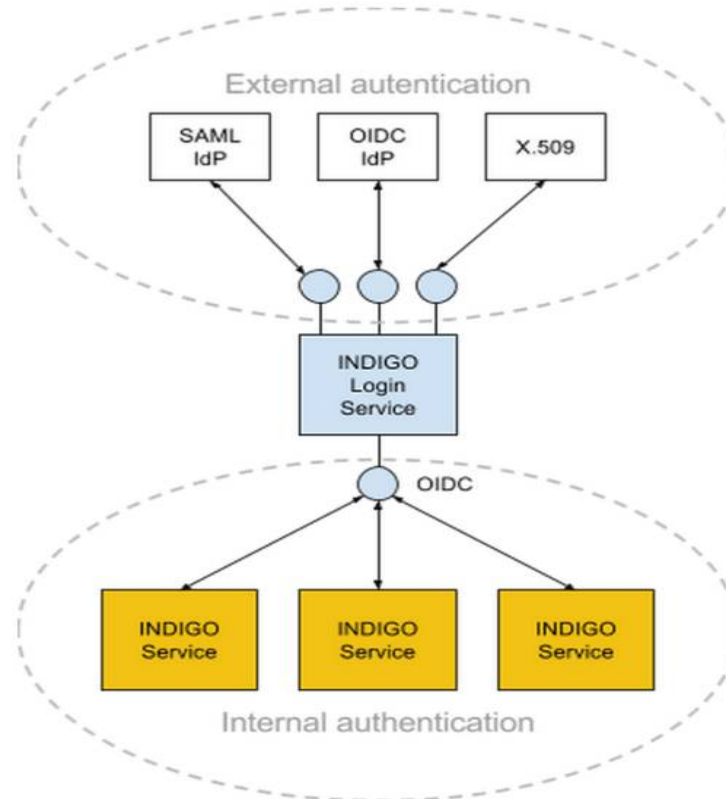
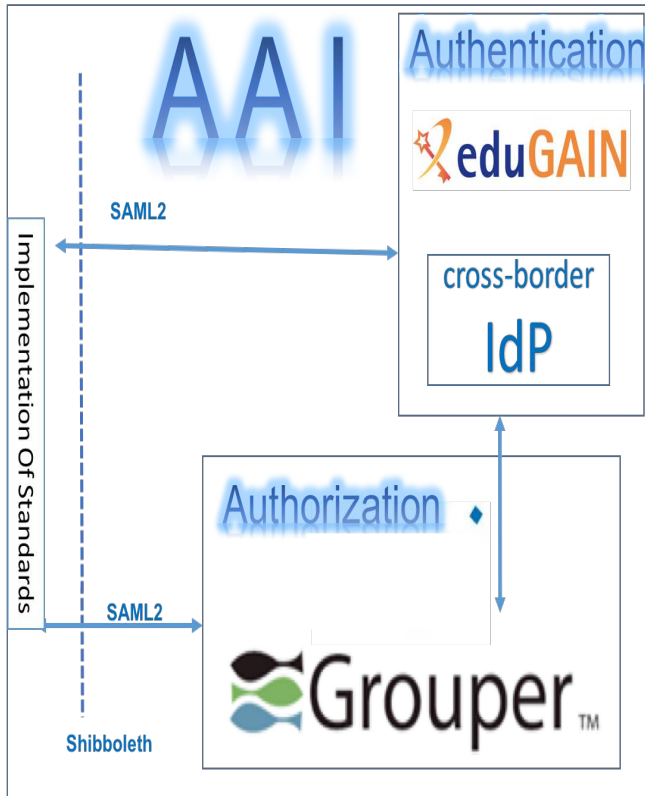
Requirements refer to a enterprise solution.

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

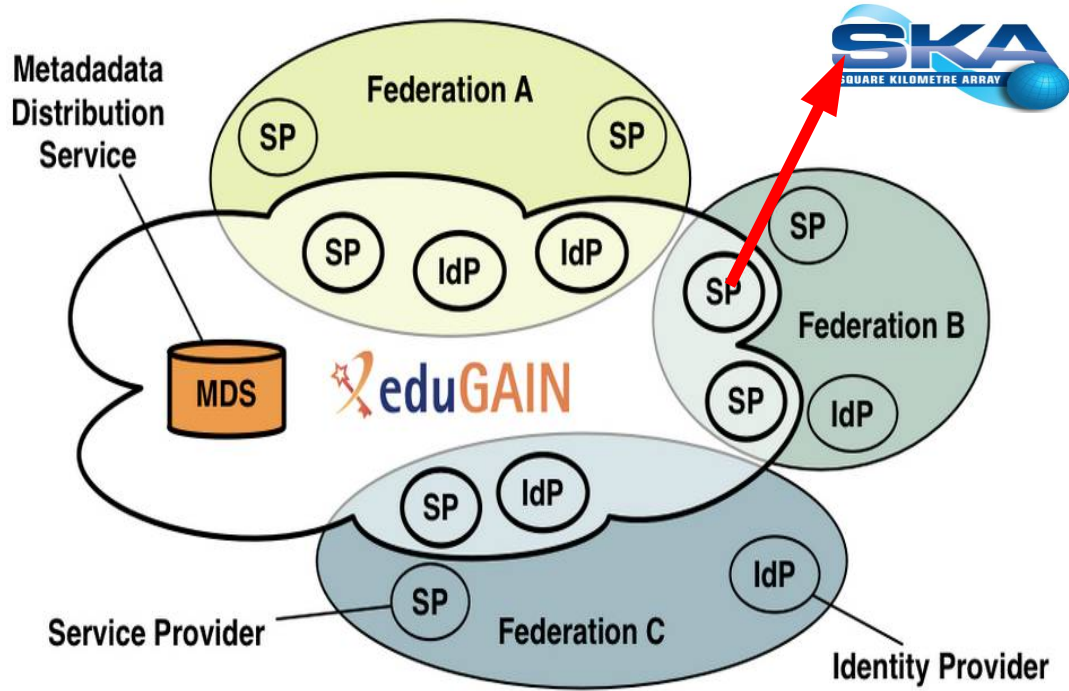
SKA and the SDC



AAA H2020 solutions



Current idea for Authentication



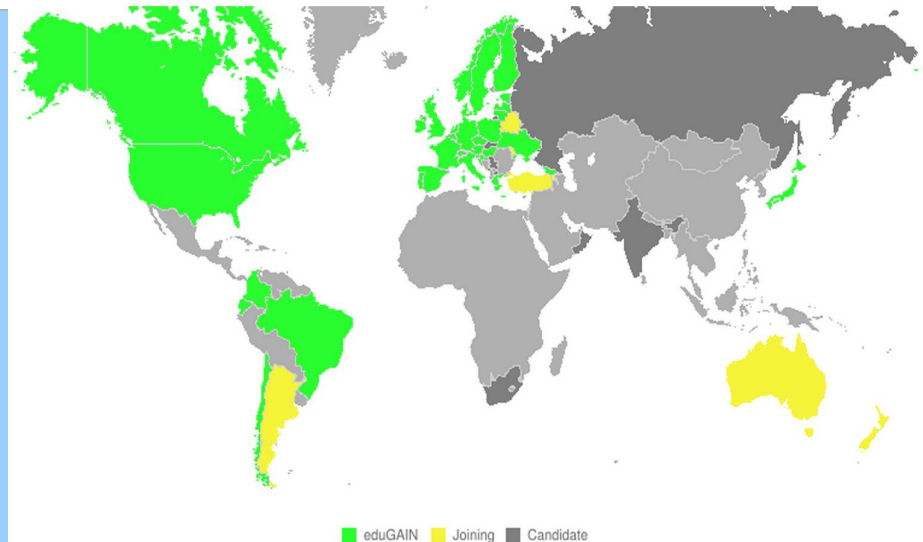
First step: implement a SERVICE provider for SKA means being able to authenticate identities already present in EduGAIN.

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)

eduGAIN membership status

Global



SKA SQUARE KILOMETRE ARRAY
TELESCOPE MANAGEMENT A&A

TELESCOPE MANAGER

TM A&A
HELP
FAQ
PRIVACY
REGISTER
LOGIN
A&A Federations
EDUGAIN

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

TM A&A

HOME

FAQ

PRIVACY

LOGIN

A&A Federations

EDUGAIN

ACCESS

TELESCOPE MANAGER USER REGISTRATION

First name: ?

Last name: ?

E-Mail: ?

Reenter E-Mail: ?

Country: ?

Institution: ?

Department: ?

Phone: ?

Mobile: ?

USER ACCOUNT

Username: ?

Password: ?

Reenter Password: ?

TM A&A

HOME

FAQ

PRIVACY

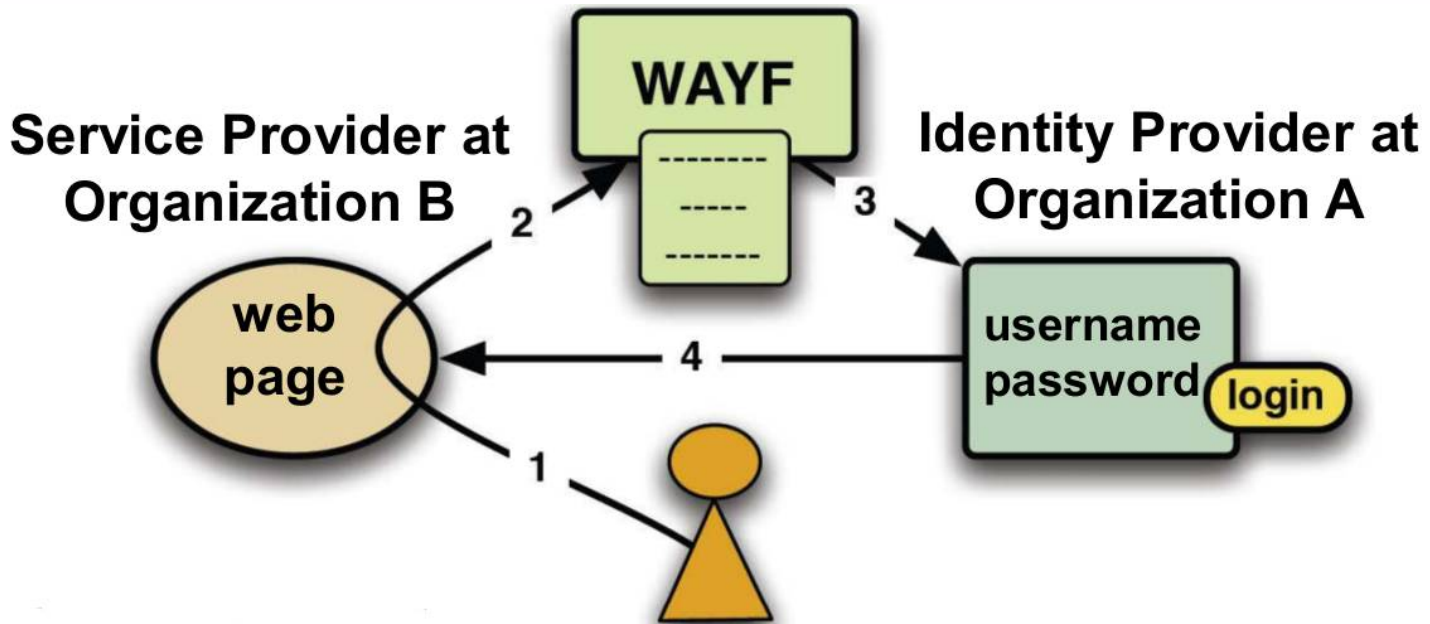
REGISTER

A&A Federations

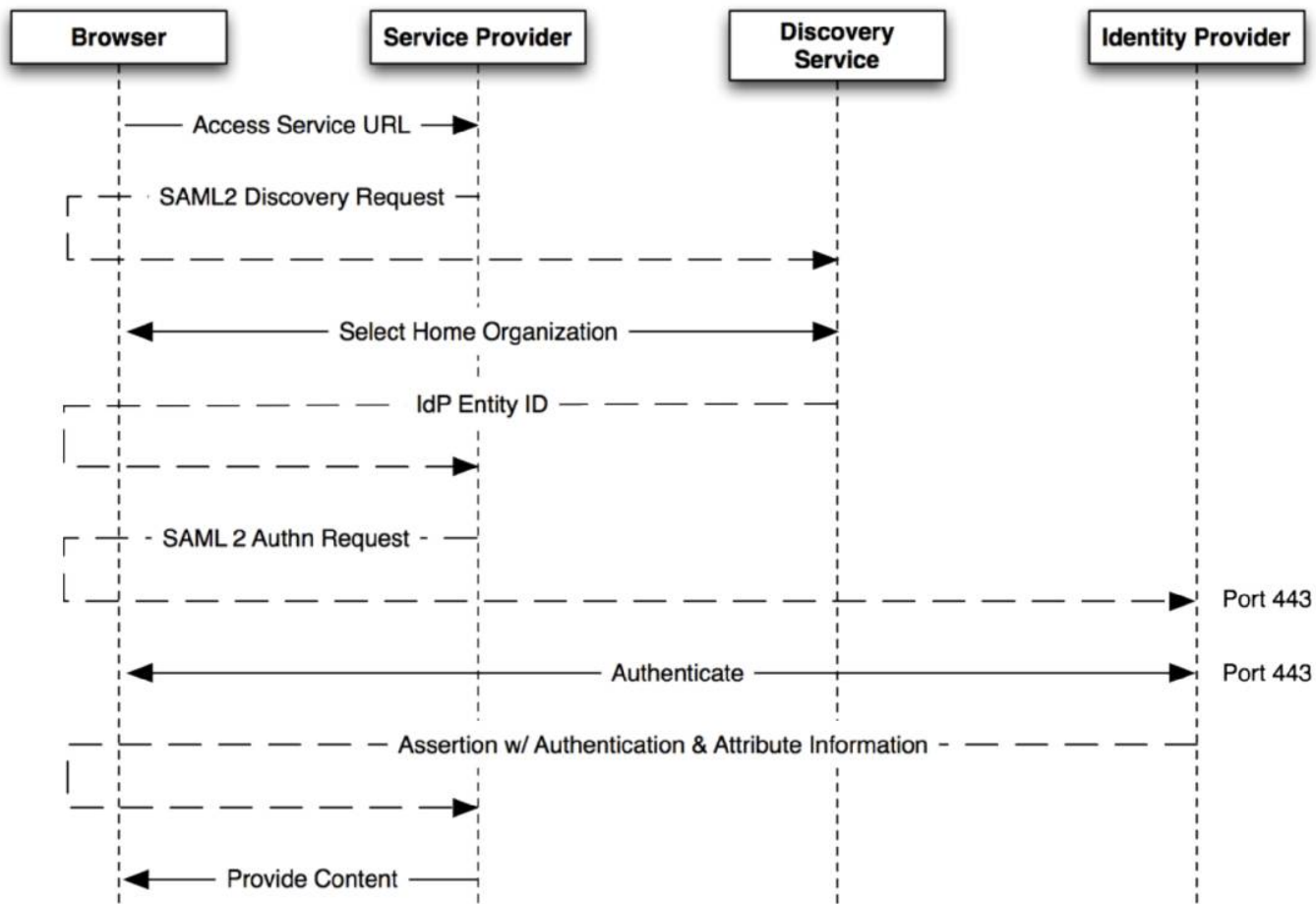
EDUGAIN

TELESCOPE MANAGER LOGIN

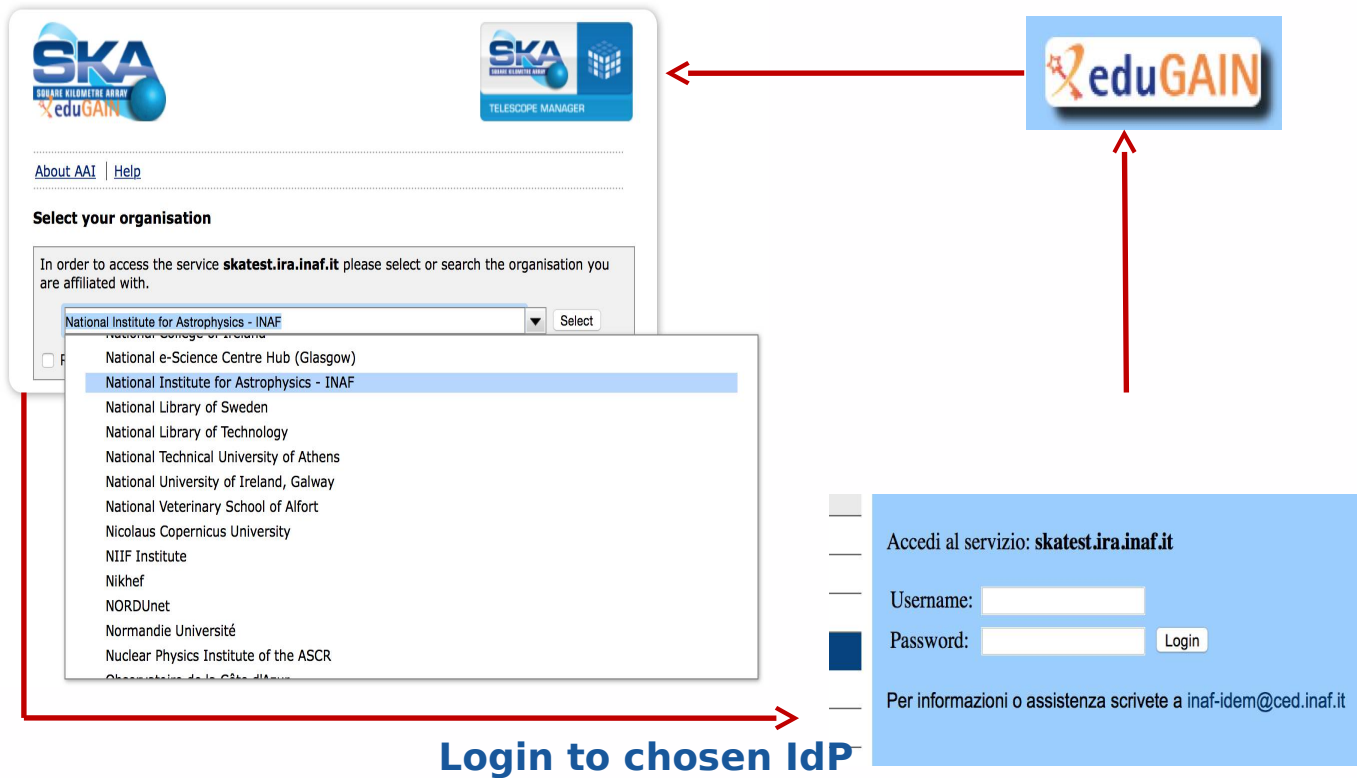
Username: Password:



Where Are You From (WAYF)



WAYF and Federated Authentication mechanism



Login to chosen IdP

TM A&A	TELESCOPE MANAGER USER REGISTRATION
HOME	First name: <input type="text" value="Franco"/> ?
FAQ	Last name: <input type="text" value="Tinarelli"/> ?
PRIVACY	E-Mail: <input type="text" value="f.tinarelli@ira.inaf.it"/> ?
LOGIN	Country: <input type="text" value="Choose country"/> ?
A&A Federations	Institution: <input type="text" value="Istituto Nazionale di Astrofisica (INAF)"/> ?
EDUGAIN	Department: <input type="text" value="IRA"/> ?
ACCESS	Phone: <input type="text"/>
	Mobile: <input type="text"/>
	<input type="button" value="Send"/>

SKA Authorization: existing and future plans

TM MANAGER
LOGOUT
PROPOSAL
SUBMIT
PROFILE
READ

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!

First step: basic authorization.

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

TM MANAGER
LOGOUT
USERS
LIST
DELETE
MODIFY
ADD
GROUPS
LIST
DELETE
MODIFY
ADD
LEVELS

USERS: SELECT OR SEARCH A USER TO MODIFY
(Fields marked with a red dot are mandatory)

User:

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

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

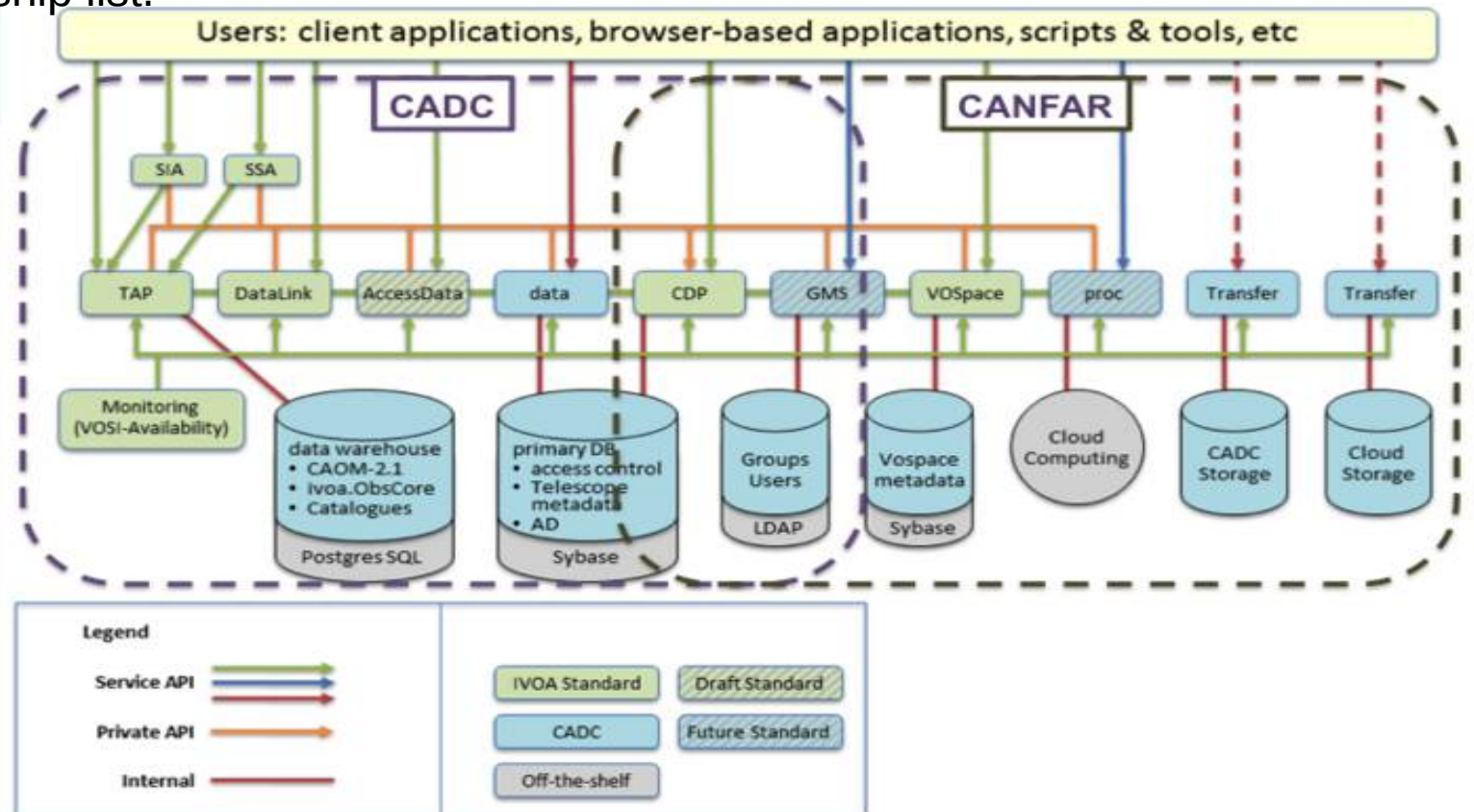
GMS solution

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

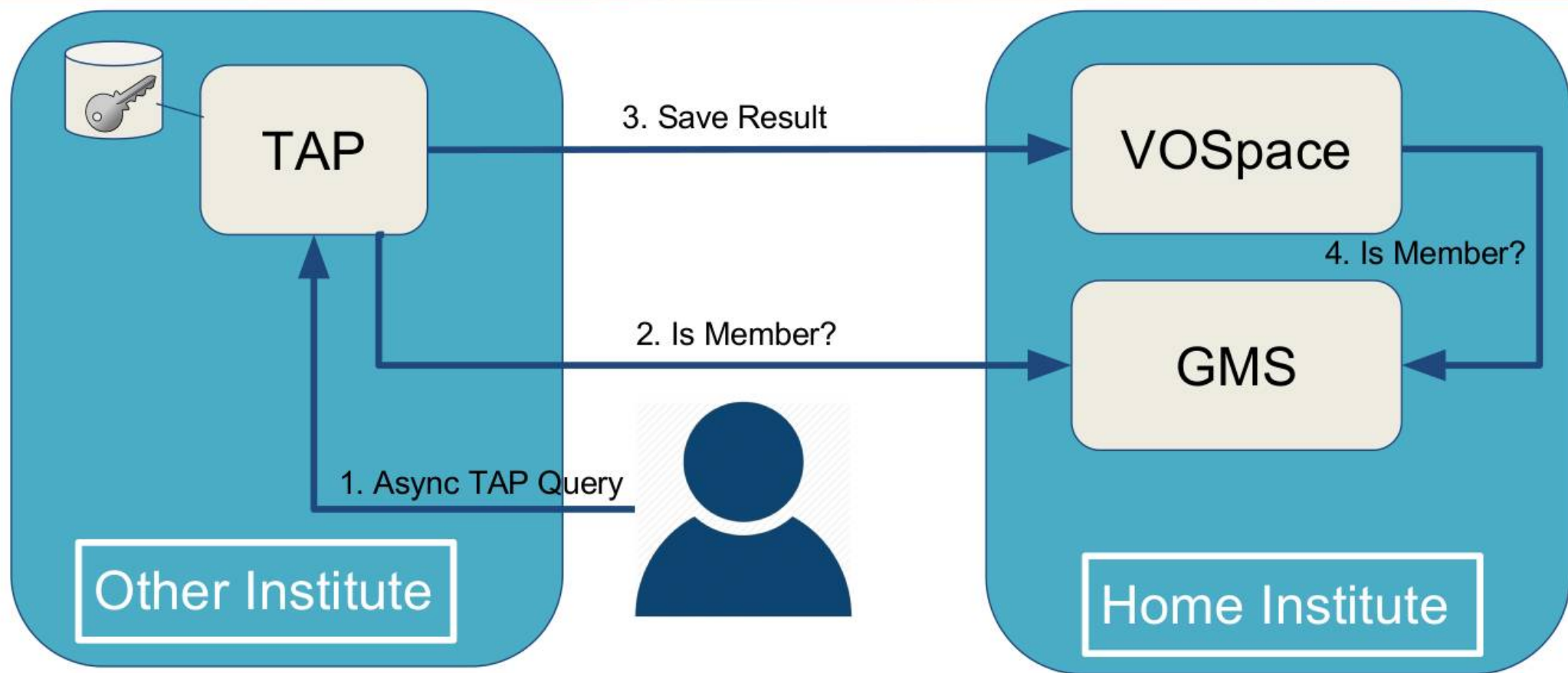
– Group Members identified with their X.509 Distinguished Name Ex:
CN=Adrian Damian,OU=hia.nrc.ca,O=Grid,C=CA

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



GMS federation mechanism

Use Case 3: Remote TAP Result Storage



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!