A&A prototype for the SKA

Cristina Knapic, Franco Tinarelli

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
  - Based on Federations (SAML2.0) but able to handle also other kind of protocols (OpenID, OAuth, ...)
- Authorization service
  - available to all SKA elements
  - 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.

AuthN and AuthZ prototype

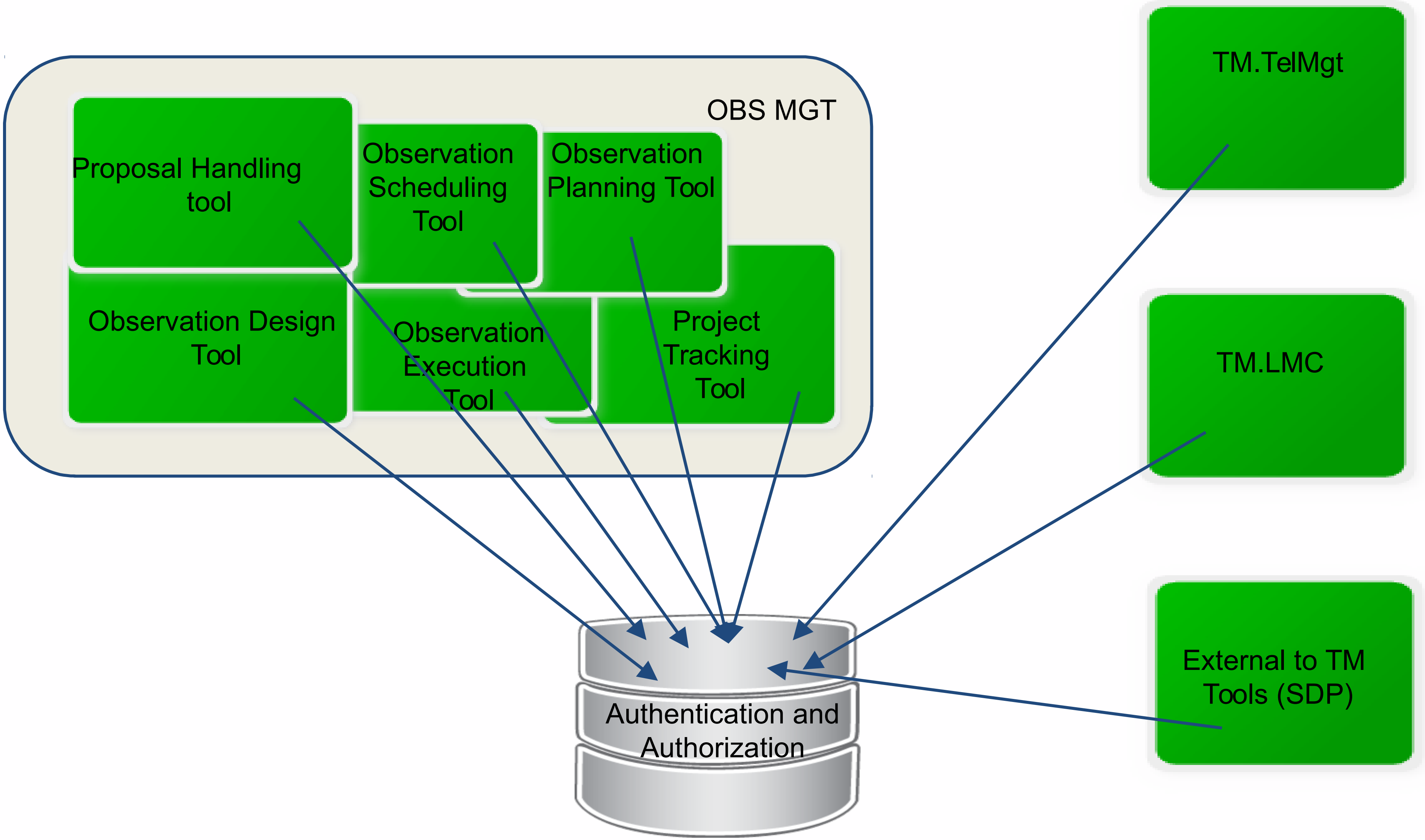
Purpose

The scope of the prototype is to implement all the functionalities necessary to identify a digital identity using self registration or federated recognition of users. This prototype is useful to investigate technological solution fitting the requirements as well as give the ability to the above tools to implement their own prototype fulfilling all the requirements related to identity recognition.

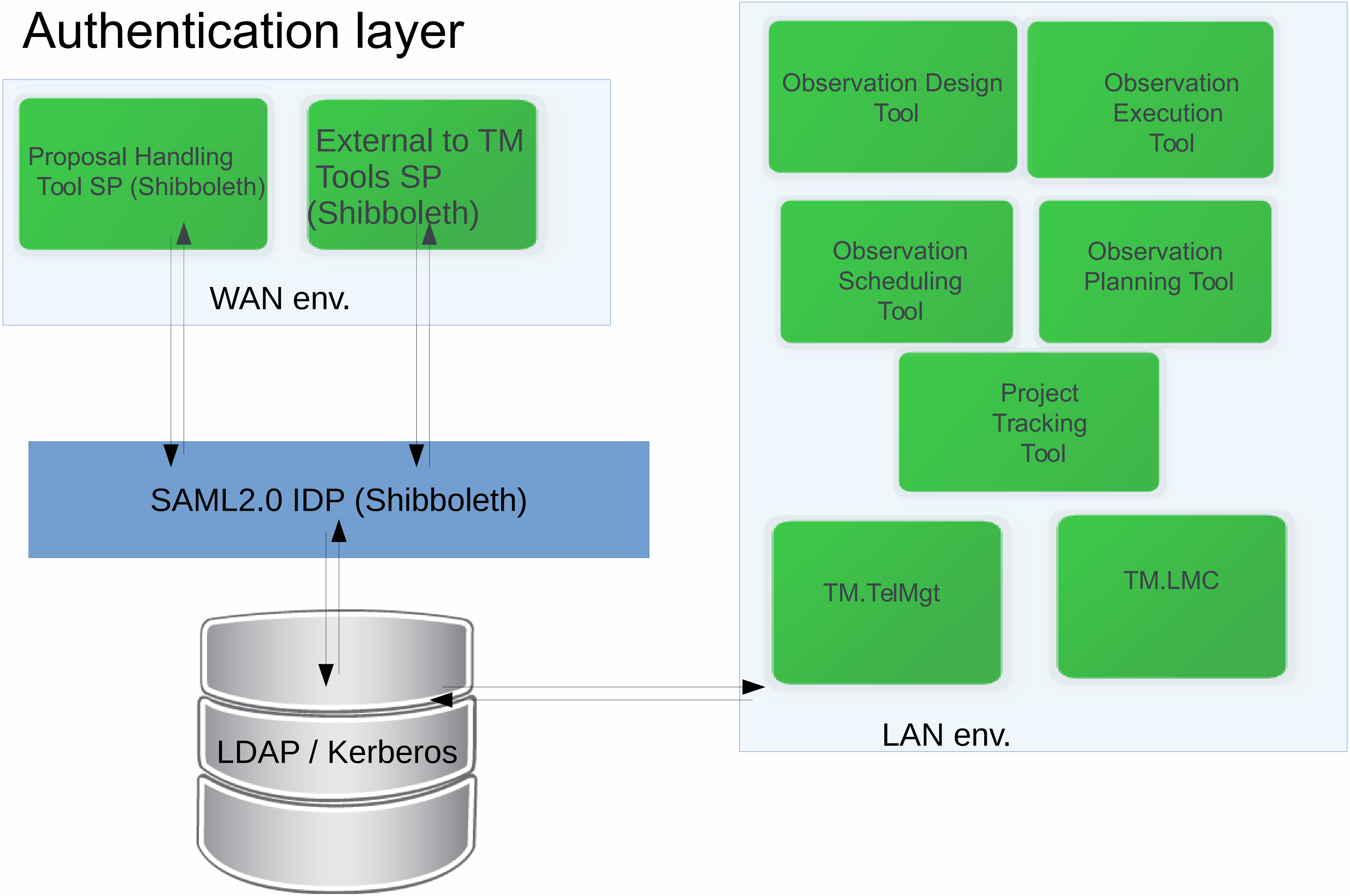
Objectives

* test technologies used for the provision of the service
* study the feasibility of a AuthN system using federations (EduGain)
* test the feasibility of an AuthZ system able to satisfy the SKA Obs Mgt PHT requirements in terms of permission and roles of users
* easy acquisition of users metadata (institute, e-mail,nationality..)

Authentication and Authorization interaction


OBS MGT
Proposal Handling tool
Observation Scheduling Tool
Observation Planning Tool
Observation Design Tool
Observation Execution Tool
Project Tracking Tool
TM.TelMgt
TM.LMC
External to TM Tools (SDP)
Authentication and Authorization

Authentication layer


Proposal Handling Tool SP (Shibboleth)
External to TM Tools SP (Shibboleth)
WAN env.
SAML2.0 IDP (Shibboleth)
LDAP / Kerberos
Observation Design Tool
Observation Execution Tool
Observation Scheduling Tool
Observation Planning Tool
Project Tracking Tool
TM.TelMgt
TM.LMC
LAN env.

Lessons learned from IDEM

- **Ide**ntity **M**anagement (IDEM) for the Italian Institutions federation: Lightweight Directory Access Protocol (LDAP) as source system
- Shibboleth use as Security Assertion Markup Language (SAML) implementation for Identity (IDP) and Service (SP) Providers.

Some considerations on the A&A system

- Degradation in performances or bottle neck if A&A mechanism is used for all the TM activities? Each PI request require a WAYF at first sign in, not the same for server machine access (local access) but what happens in case of net outage?
- Performances at submission deadlines for the ObsMgt PST could became critical? Dependence on IDP reliability?
- Evolution of requirements during the life ?
- Portability on other technologies could be affected by architectural choices (OpenId instead of SAML) if no layers like Unity are build over it ?
- How to automatically handle the merging of different identities for the same physical person?

A&A prototype

Approach: Implementation of existing technologies

Technology Stack

PHP, Shibboleth, LDAP, MySQL, Java

A&A Technology Stack

Easily handlable interpreted language. It could run from the command line.
WEB APPLICATION

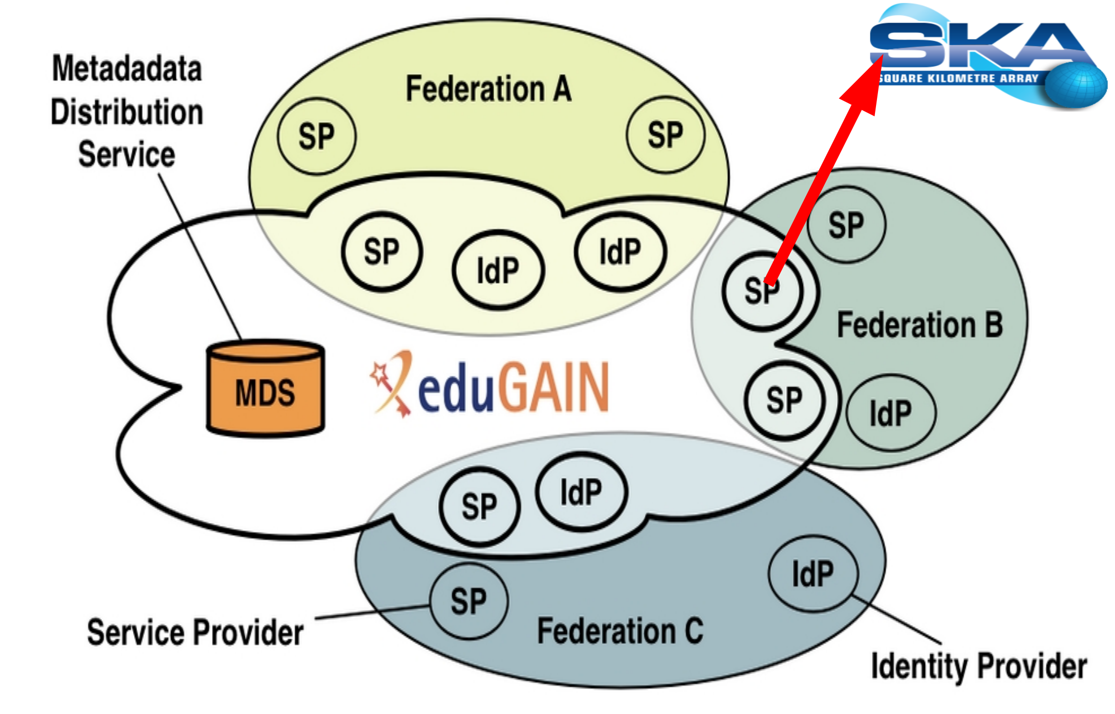
Open source management system. **DATA BASE MANAGER**

Open-source project providing Single Sign On utilities, allowing access to on line resources. **IDENTITY e SERVICE PROVIDER**

Security Assertion Markup Language, protocol XML based that uses tokens To exchange informations between IdP e SP. **A&A**

Where Are You From: tool developed by Switch for choosing the reference IdP. **WAYF**

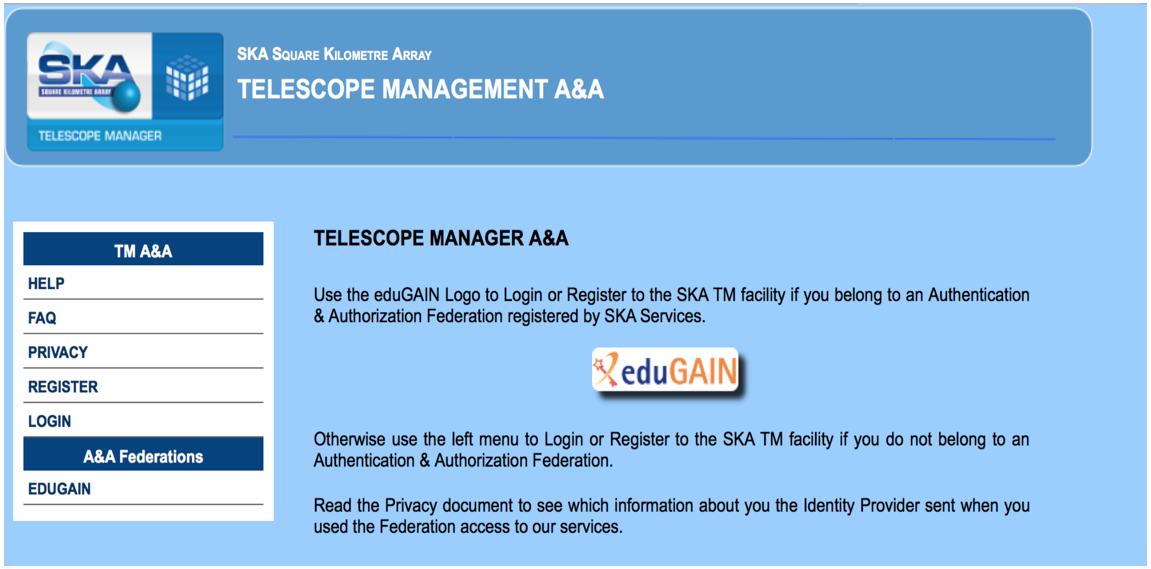
Current idea for Authentication



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

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.

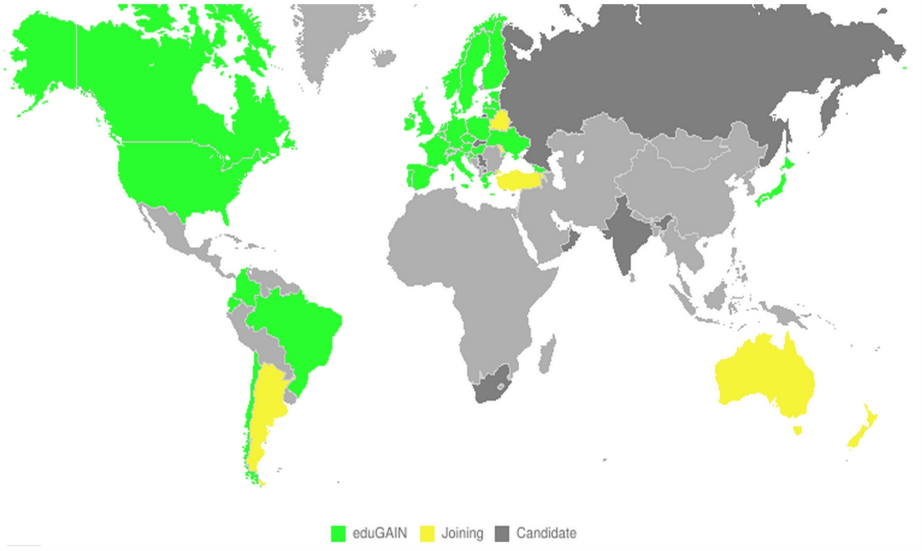
eduGAIN

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

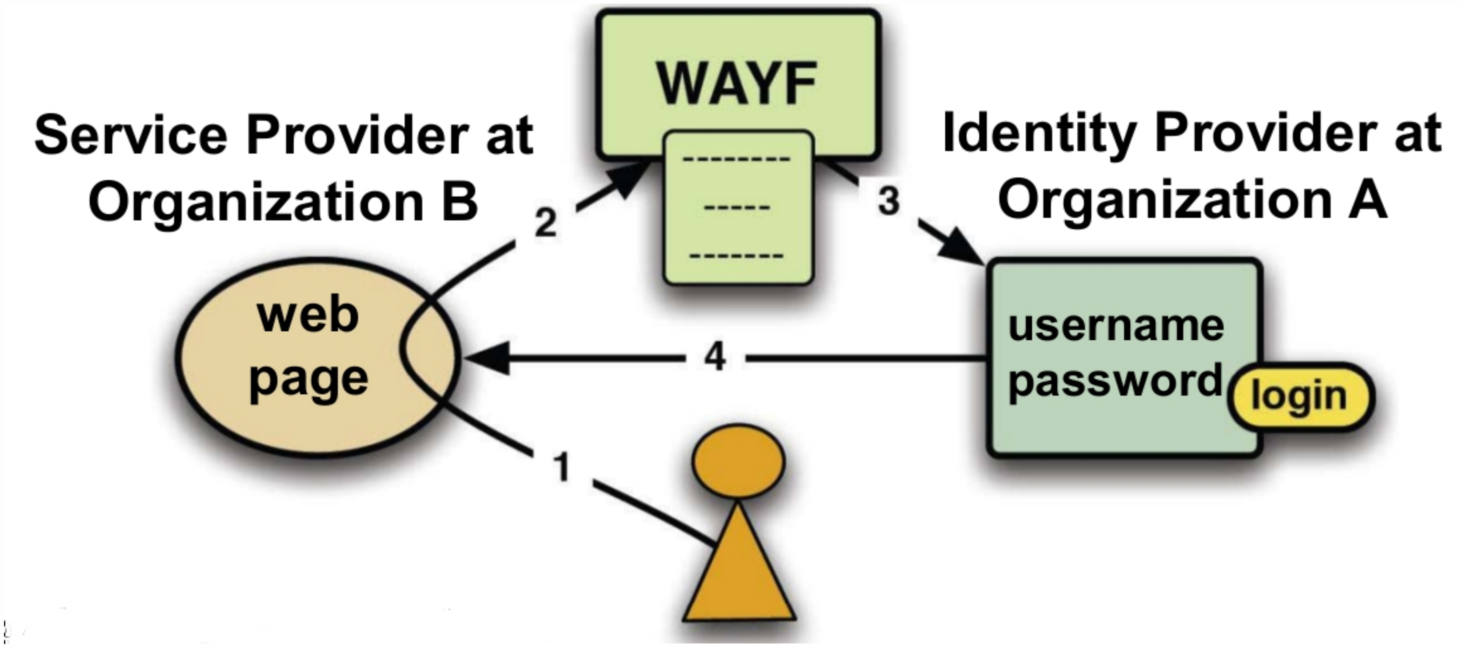
Read the Privacy document to see which information about you the Identity Provider sent when you used the Federation access to our services.

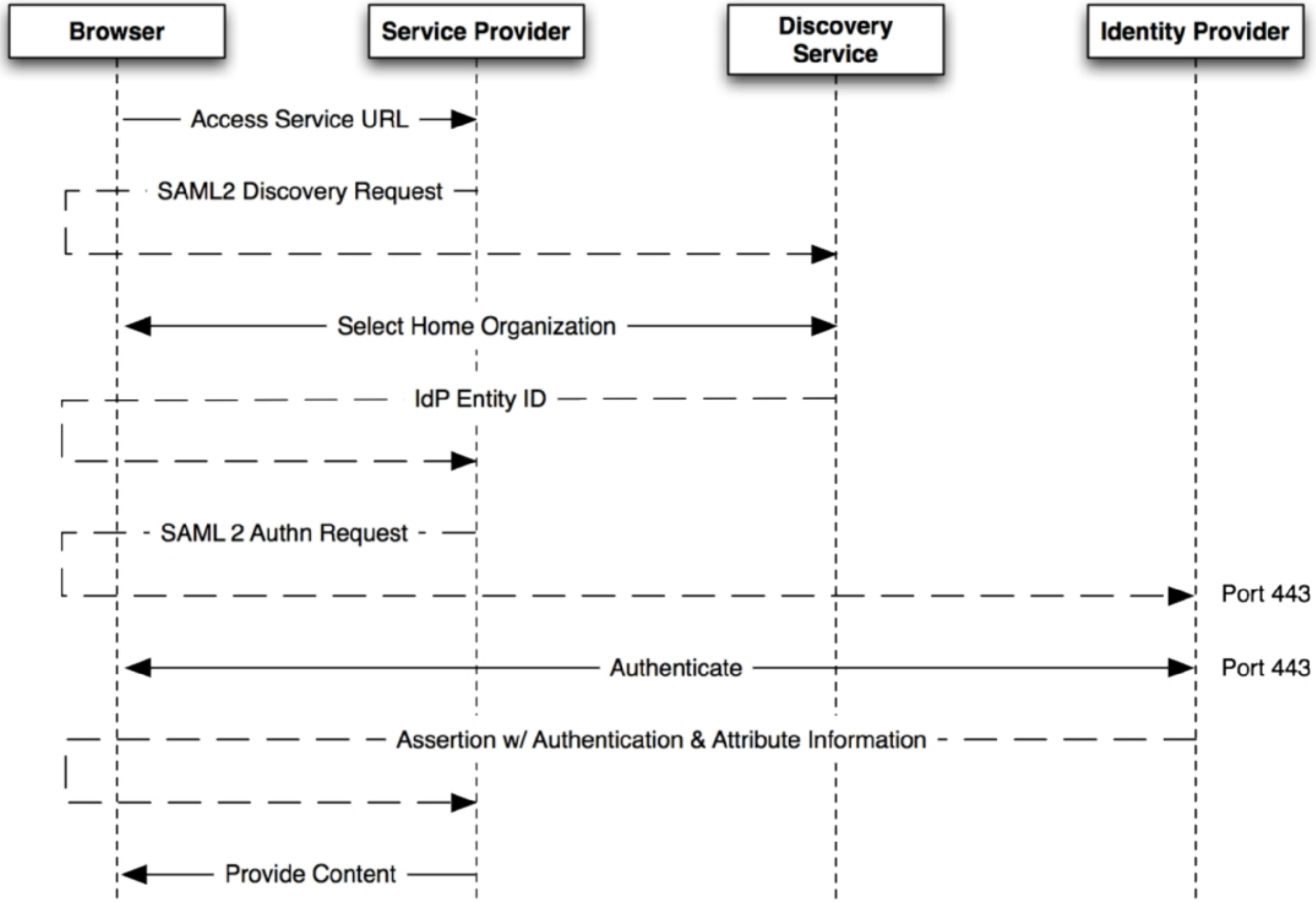
eduGAIN membership status

Global

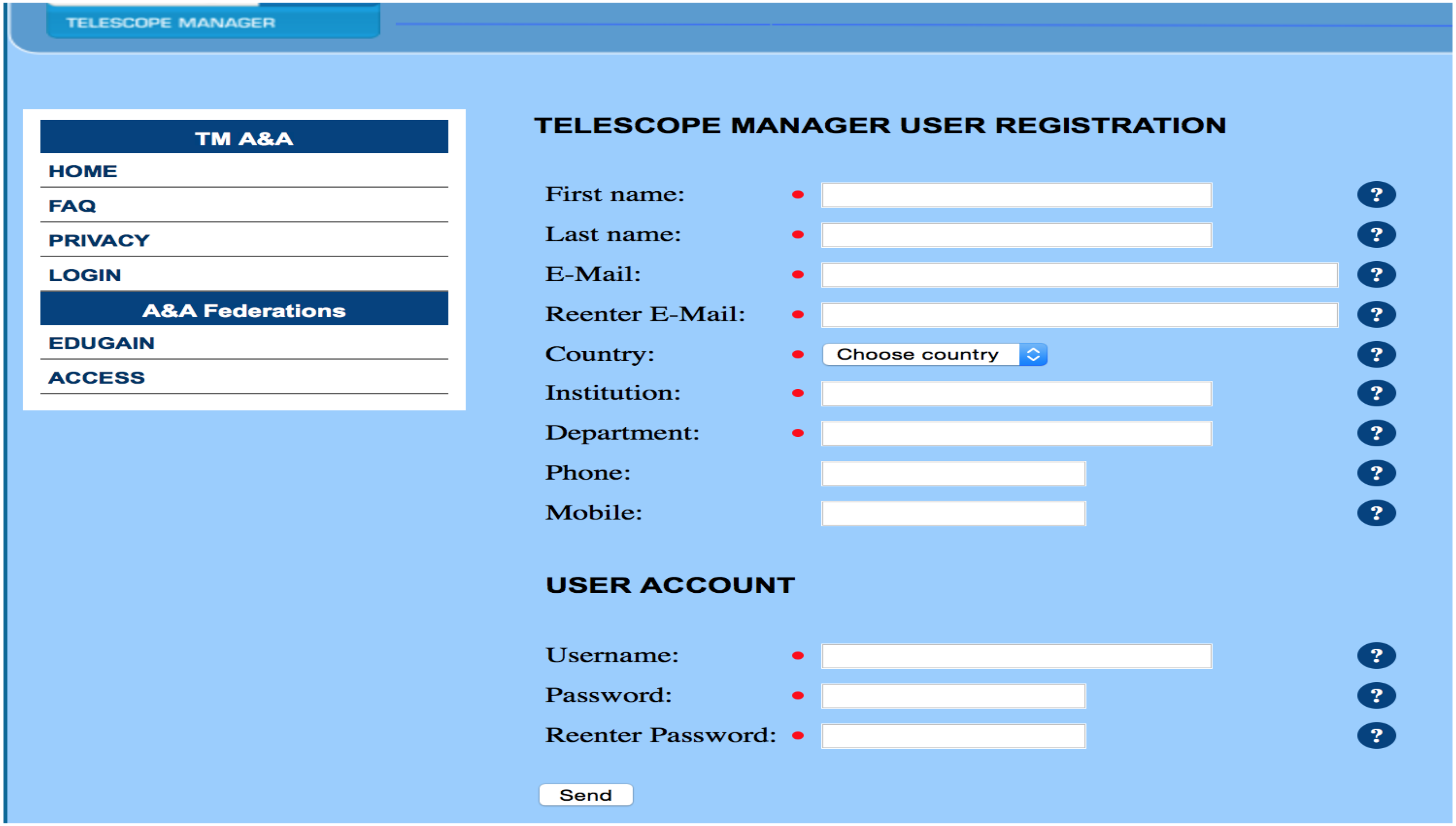


Where Are You From (WAYF)


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



Self registration Authentication mechanism

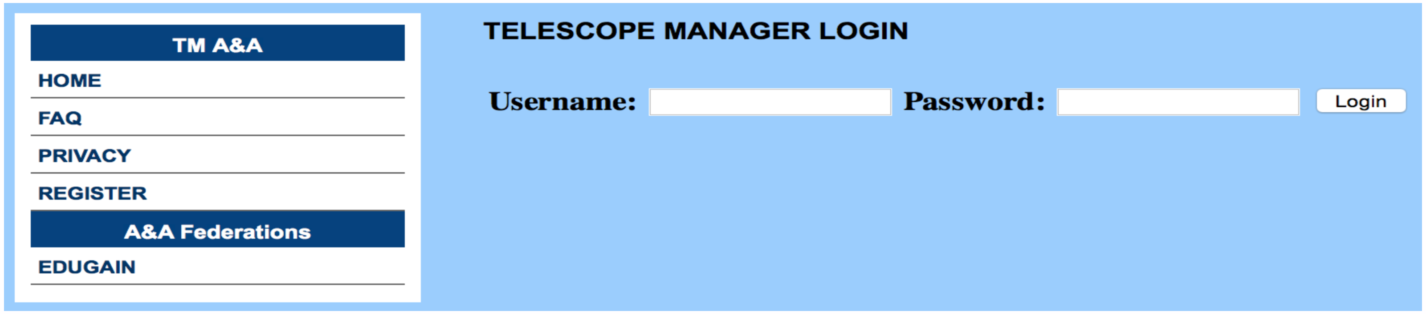


TELESCOPE MANAGER USER REGISTRATION

First name:	●	?
Last name:	●	?
E-Mail:	●	?
Reenter E-Mail:	●	?
Country:	● Choose country	?
Institution:	●	?
Department:	●	?
Phone:		?
Mobile:		?

USER ACCOUNT

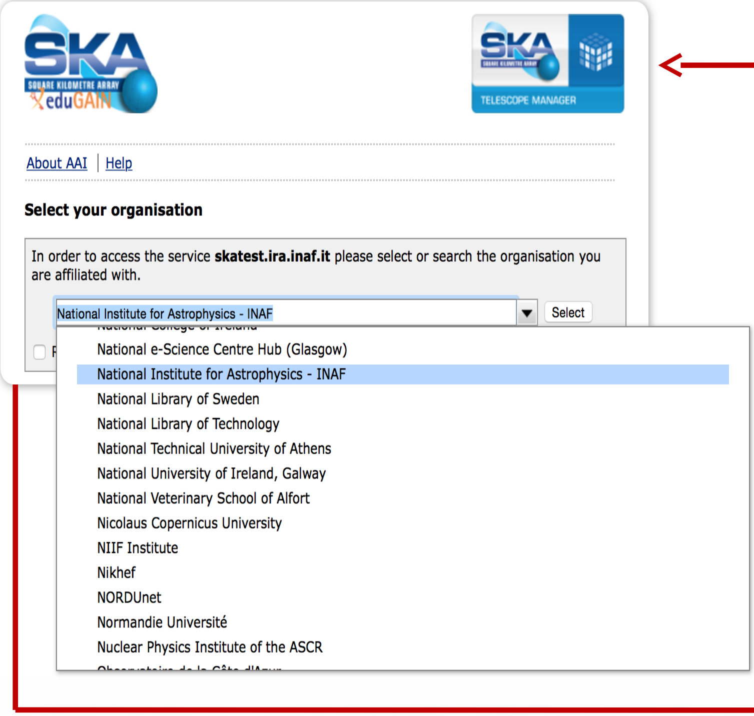
Username:	●	?
Password:	●	?
Reenter Password:	●	?



TELESCOPE MANAGER LOGIN

Username: Password:

WAYF and Federated Authentication mechanism



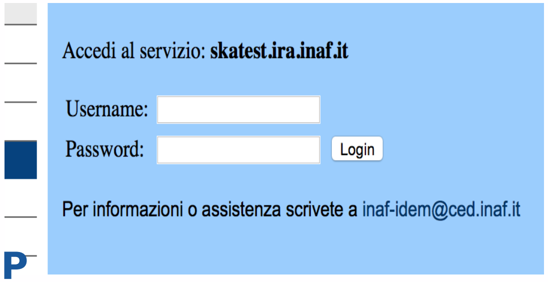
Select your organisation

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

□ F

- 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



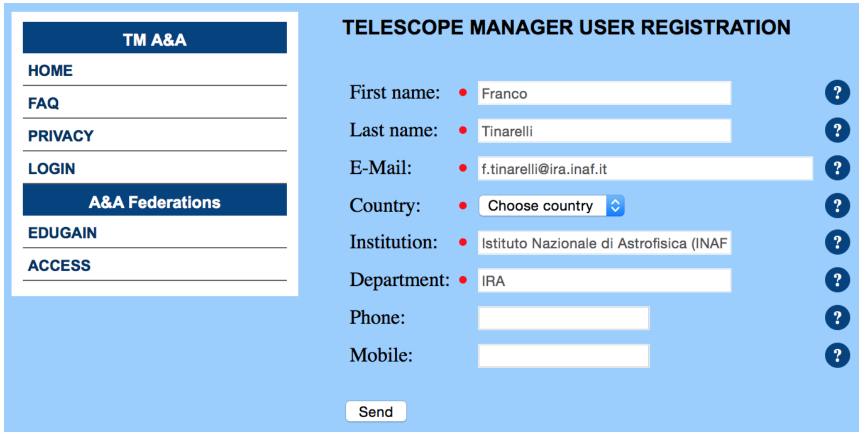
Accedi al servizio: **skatest.ira.inaf.it**

Username:

Password: Login

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

Login to chosen IdP

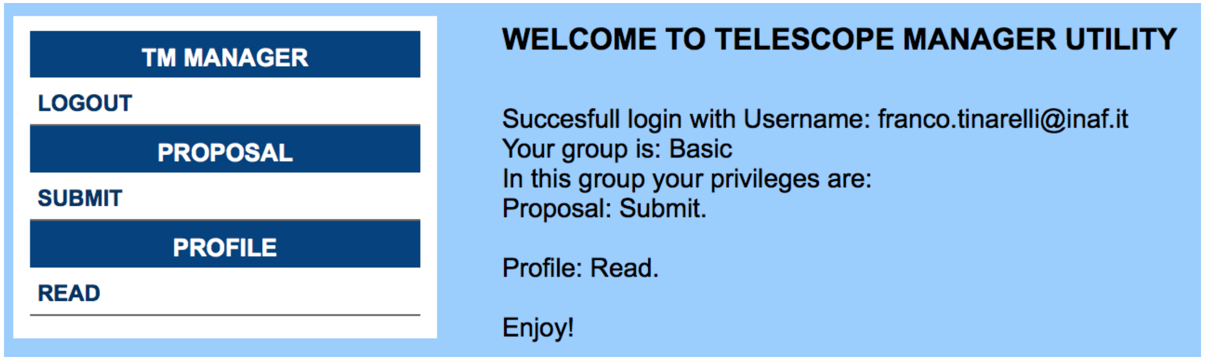


TELESCOPE MANAGER USER REGISTRATION

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

Authorization mechanism



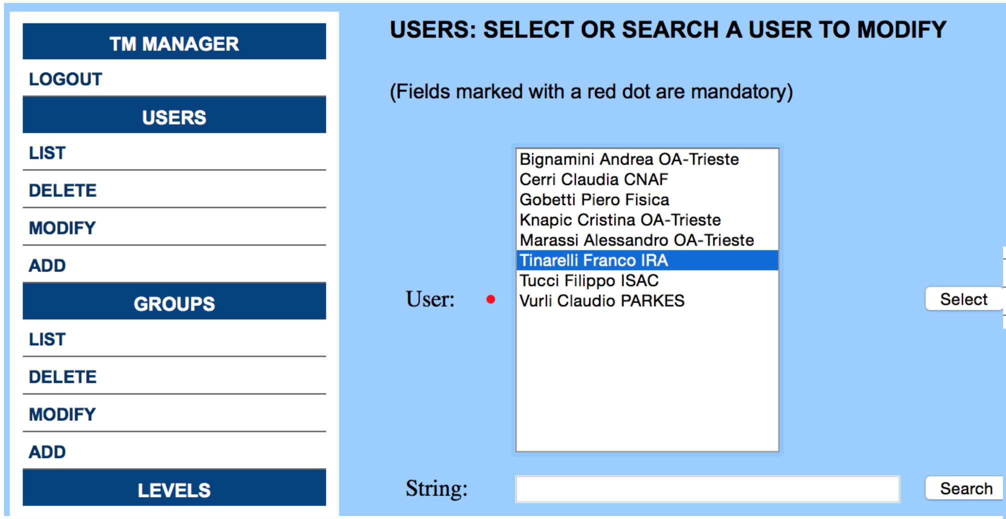
WELCOME TO TELESCOPE MANAGER UTILITY

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.



USERS: SELECT OR SEARCH A USER TO MODIFY

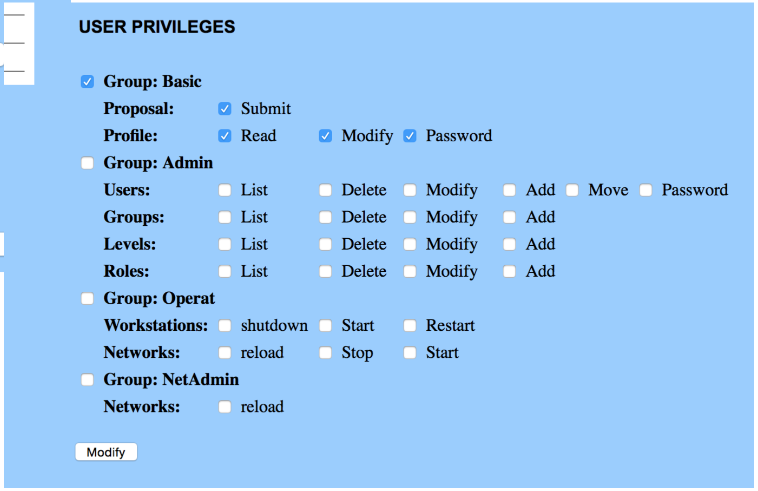
(Fields marked with a red dot are mandatory)

User: ●

Bignamini Andrea OA-Trieste
Cerri Claudia CNAF
Gobetti Piero Fisica
Knapic Cristina OA-Trieste
Marassi Alessandro OA-Trieste
Tinarelli Franco IRA
Tucci Filippo ISAC
Vurli Claudio PARKES

String:

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



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

Thank you for your attention!

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