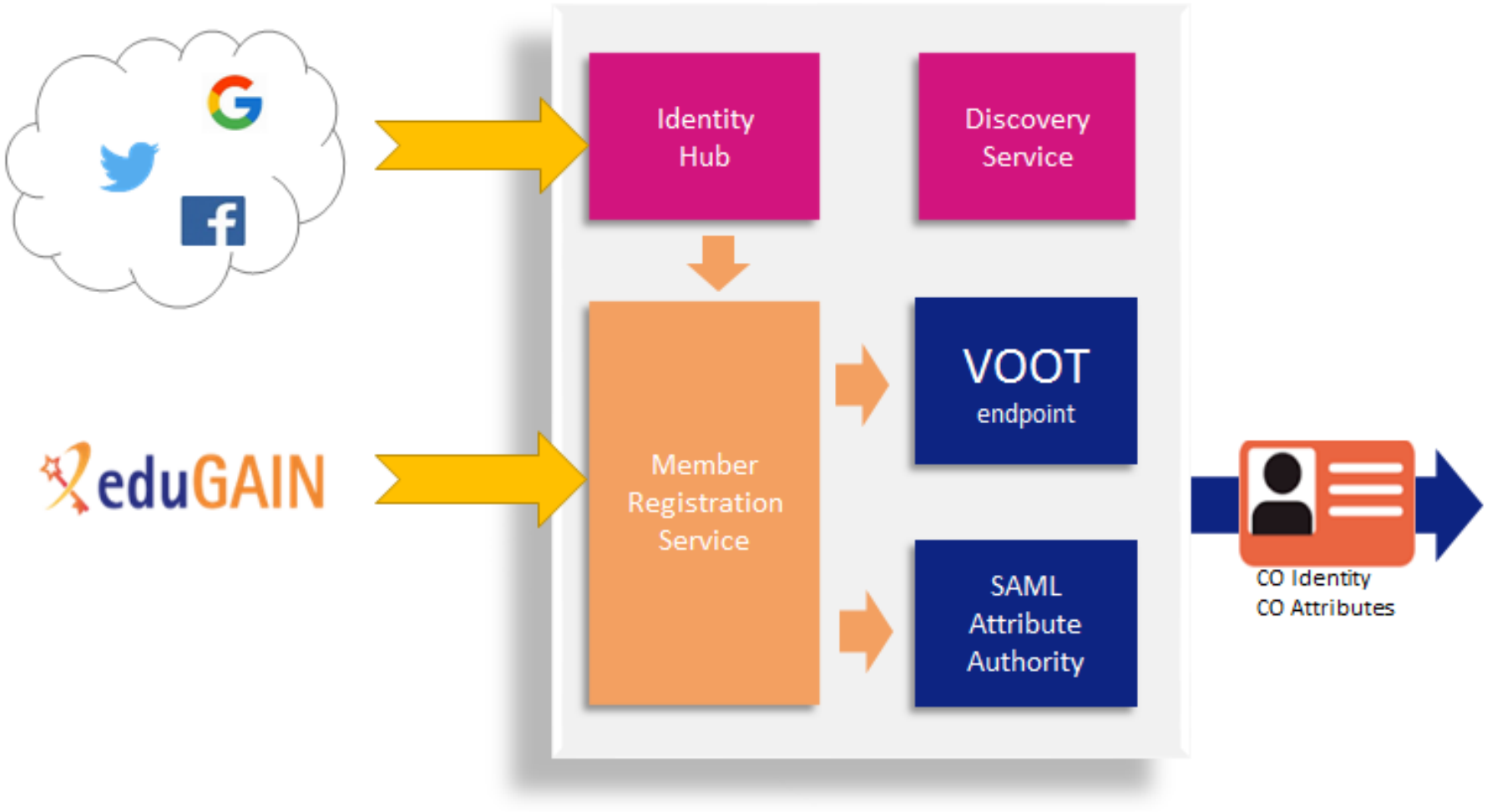
Authentication

Shih, A. Haigron, R. Le Sidaner, P.

IVOA Interop, Santiago 27-29/10/2017

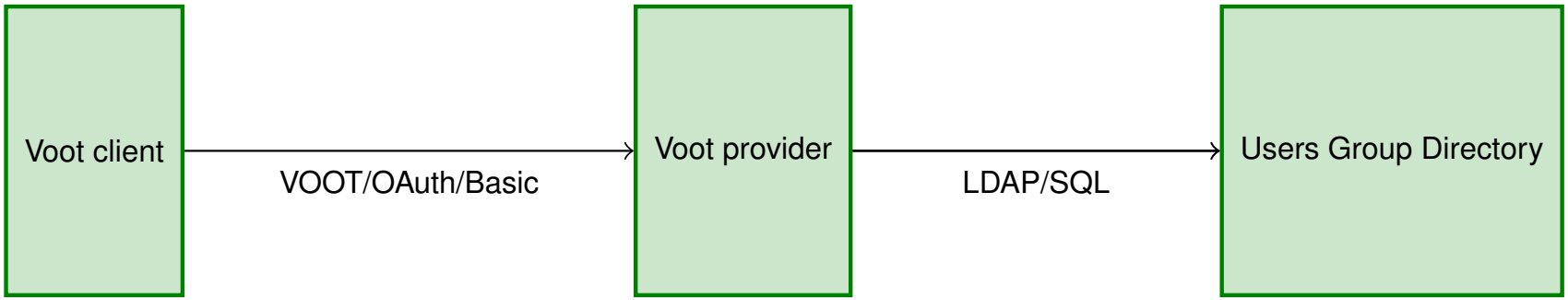
EDUTEAM


Identity Hub
Discovery Service
eduGAIN
Member Registration Service
VOOT endpoint
SAML Attribute Authority
CO Identity
CO Attributes

Eduteams and Geant. . . is it THE solution for IVOA?

- We met Chris Atherton from GEANT at EPSC in Riga.
- He propose us to have look at Eduteam.
- `https://wiki.geant.org/display/gn42jra3/eduTEAMS`
- `https://www.geant.org/Innovation/eduteams/Pages/How-eduTEAMS-works.aspx`
  - Membership management, Identity Hub for non eduGAIN users, Basic Groups, and Basic Provisioning.
  - allows end users of eduGAIN members to be able to login.
  - has infrastructure operation provided by GÉANT.
  - is offered to users at no additional cost.
  - allow multiple ID federation OpenID. . . .
  - propose to handle group for authorization.
  - What time scale for UP and Running solution?.
  - What Advantage in the Non Free solution?.

What we have try to handle syntax and REST method



REST API to access information

- People informations : `https://auth.obspm.fr/groups/USERID`
- Group informations : `https://auth.obspm.fr/peoples/USERID/GROUPID`

People informations

Example

group information for user lesidaner URL: `https://auth.obspm.fr/groups/lesidaner` the result are `json`

```
{"totalResults": 1,
  "entry": [
    { "description": "Group for test",
    "id": "testgroup
    }
  ]
}
```

Group informations

Example

Accessing all user for the group where lesidaner is member URL: `https://auth.obspm.fr/peoples/lesidaner/testgroup` the result are `json`

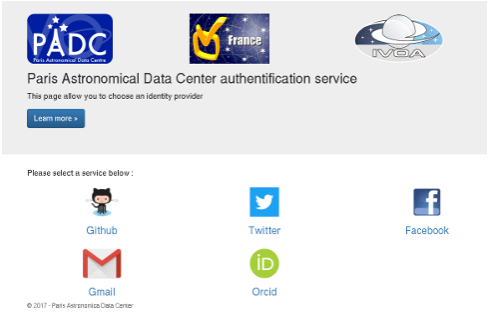

```
{ "entry": [
  { "displayname": "null",
     "mail": [
       "jas01-11524096@github_fake"
     ]
   },
   { "displayname": "nul}",
     "mail": [
       "0000-0001-9629-2922@orcid_fake"
     ]
   },
 ],
 "totalResults": 2
}
```

Using topcat and DaCHS

- We have a internal tap server (not open to all internet) `http://voparis-jpl.obspm.fr/tap`.
- We don't want to modify this application.
- We put a LDAP authenticate proxy in the front of that server, `https://voparis-srv-paris.obspm.fr/ivoa/`.
- It ask for user and password taken from integrated SSO, `https://auth.obspm.fr/`.

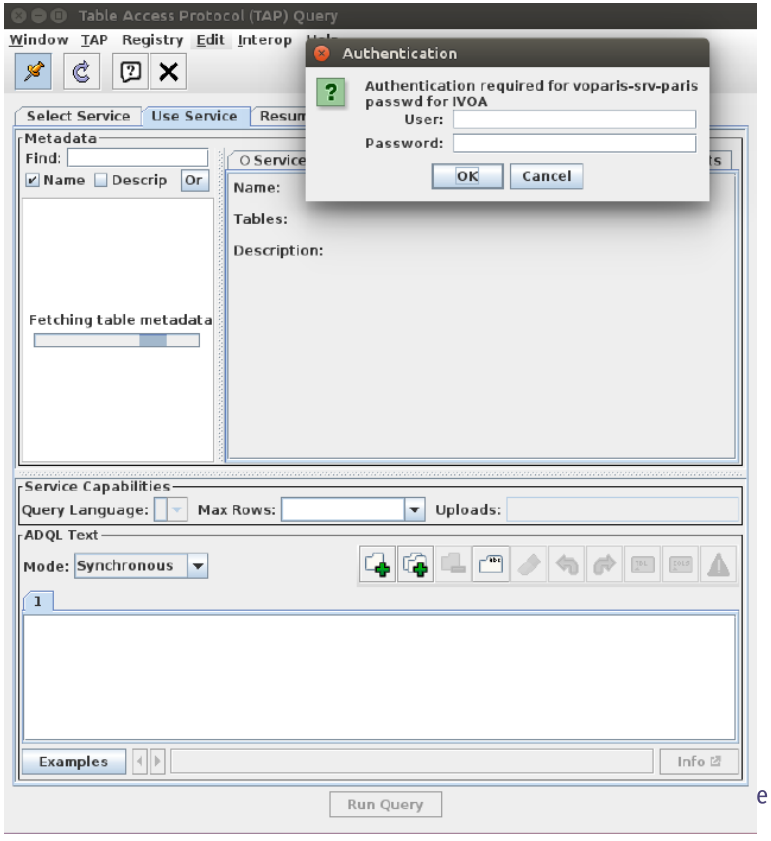
Using topcat and DaCHS

- Authentication



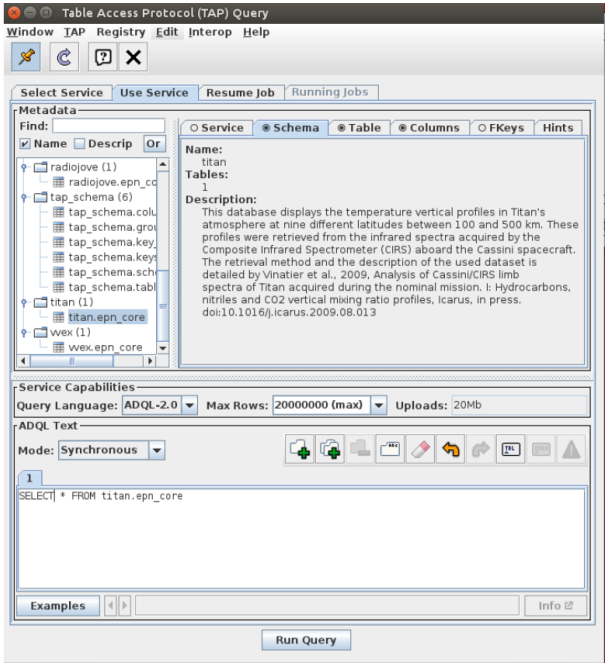
- Password

- Login in tap

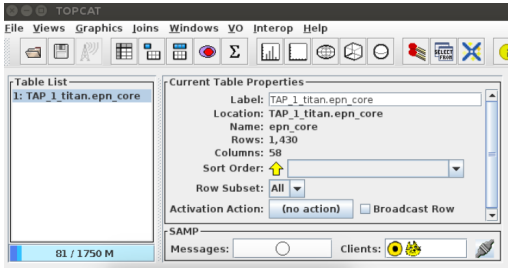


Using topcat and DaCHS

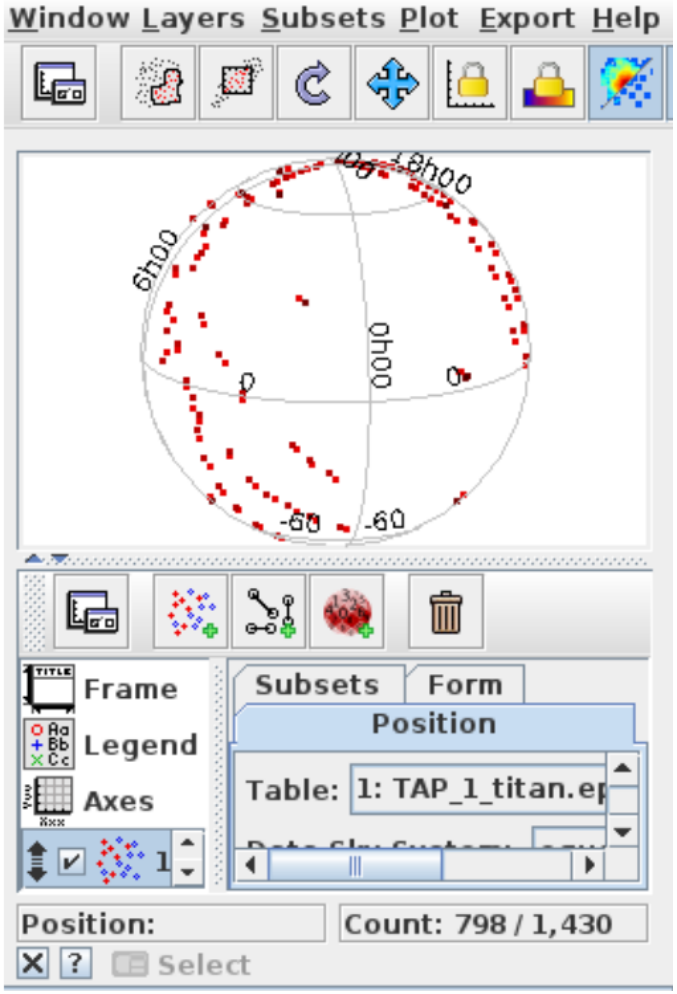
- Select



- Select



- Display



Conclusion

Does IVOA want a central Annuary?

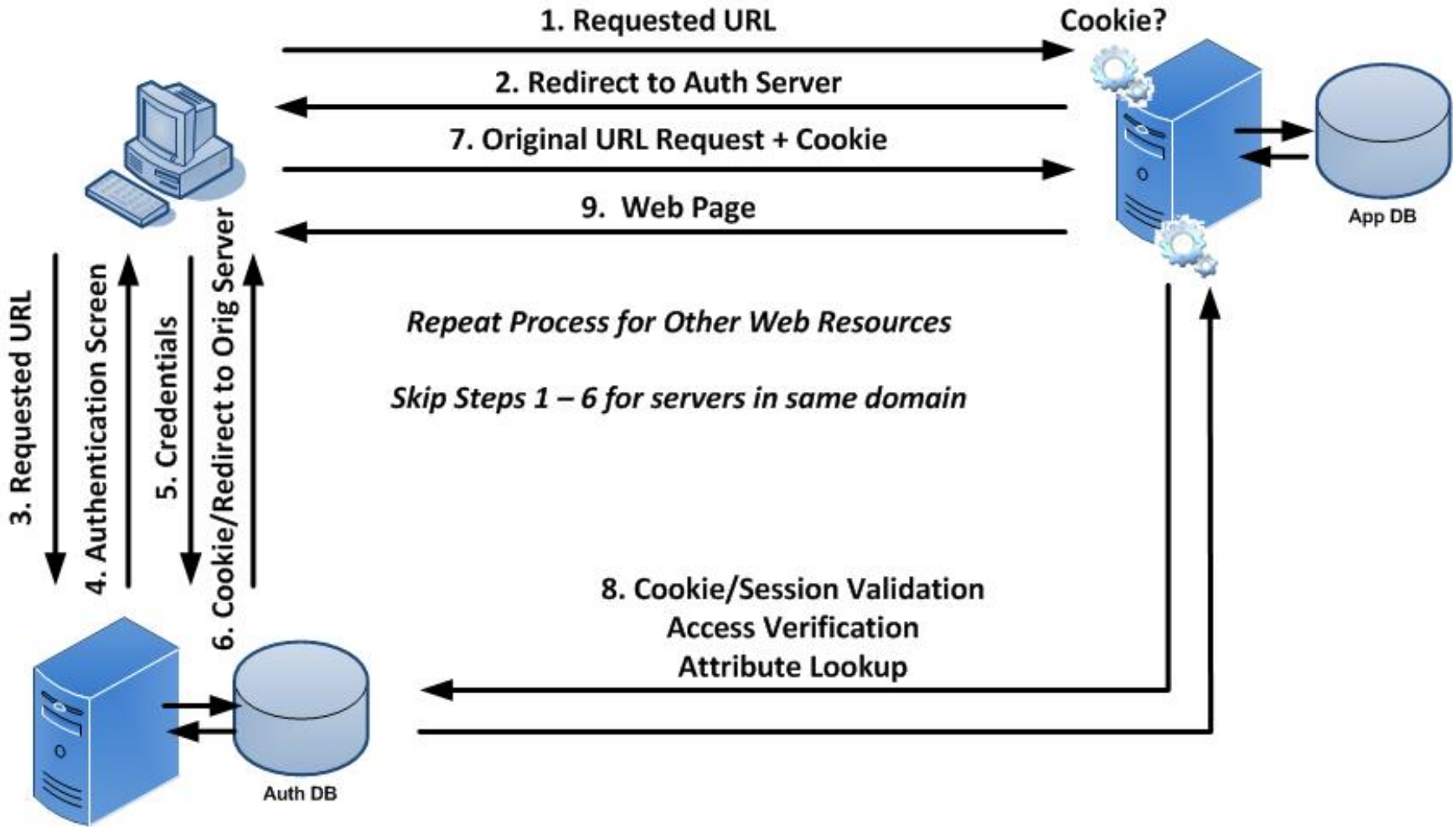
- Separate Authentication between federation and application
- Use LDAP like and delegate group administration VOOT?
- Have a centralised Authorisation system with delegation
- What link with large project CTA, SKA...

Then make convergence and delegation for next interop?

What we have try to handle last time

- Don’t want to manage people (no account creation no passwd management).
- Ability to authenticate non web application like `ssh`, `rsync` also `Aladin Topcat`.
- Ability to authenticate existent applications.
- Ability to manage easily authorizations.
- Easy to integrated in new applications and **old** applications.
- Easy to deploy.
- Easy to maintain with few manpower.
- Secure.

How SSO works



Problems

- Highly based on `http-redirect`, don't work well outside web-browser.
- Hard to use on CLI (`ssh`, etc.)
- Lots of implementation : SAML2 (shibboleth), oauth, openid, etc.
- Complex to very complex to integrate.
- Don't integrate authorizations, each application must manage it own authorizations, meaning each application provider must implement his own tools.

LDAP

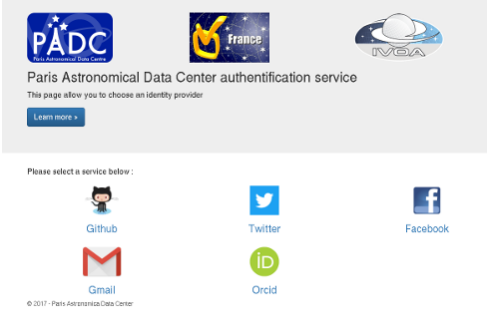
- Why
  - Use LDAP for authentication beckoned over ID Federation.
  - LDAP is well documented protocol.
  - All (almost) application can easily to use LDAP as authentication back-end.
  - Easy to use on CLI.
  - LDAP as « group » notion. Use LDAP group as authorizations back-end.
  - Easy to centralize.
- But
  - Don’t want to populate the LDAP.
  - Don’t want to manage expiration.

LDAP+SSO

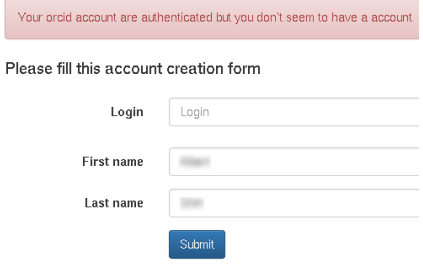
- Using SSO
- Populate a LDAP

Prototype

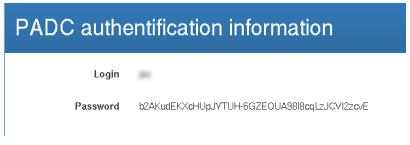
- User ask to choose a authentication service (like Orcld, Google, Github, Facebook etc.)



- If he don't have a account, we invite him to create one.



- We generate a temporary password and add it to a LDAP



Prototype

- Use this couple login/password in all your applications.
- The password is temporary same as the TTL of a cookie any web application.
- All providers can use this LDAP authentication.

Authorizations

- Easy to manage authorizations
- Create group (in LDAP) like
  `cn=myapp, ou=groups, dc=padc, dc=fr, dc=ivoa`
- Authorizations with *memberOf* test.
- For example:
  - Apache: `Require ldap-group myapplication`
  - Pam :
    `pam_filter |(member=cn=myapp,ou=groups,dc=padc,dc`
  - sshd : `Allowgroups` and `ldap.conf`

The future

- Accounts convergences :
  - Peoples who have multiple account
  - Peoples who change institution.
- Create Authorizations service.
- Delegation by branch in the LDAP.
- Delegation of the authorizations services.
- Add SAMLv2 (Shibboleth/Edugain).