

Shibboleth and OpenID at VOPDC

Mathieu Servillat, Pierre Le Sidaner

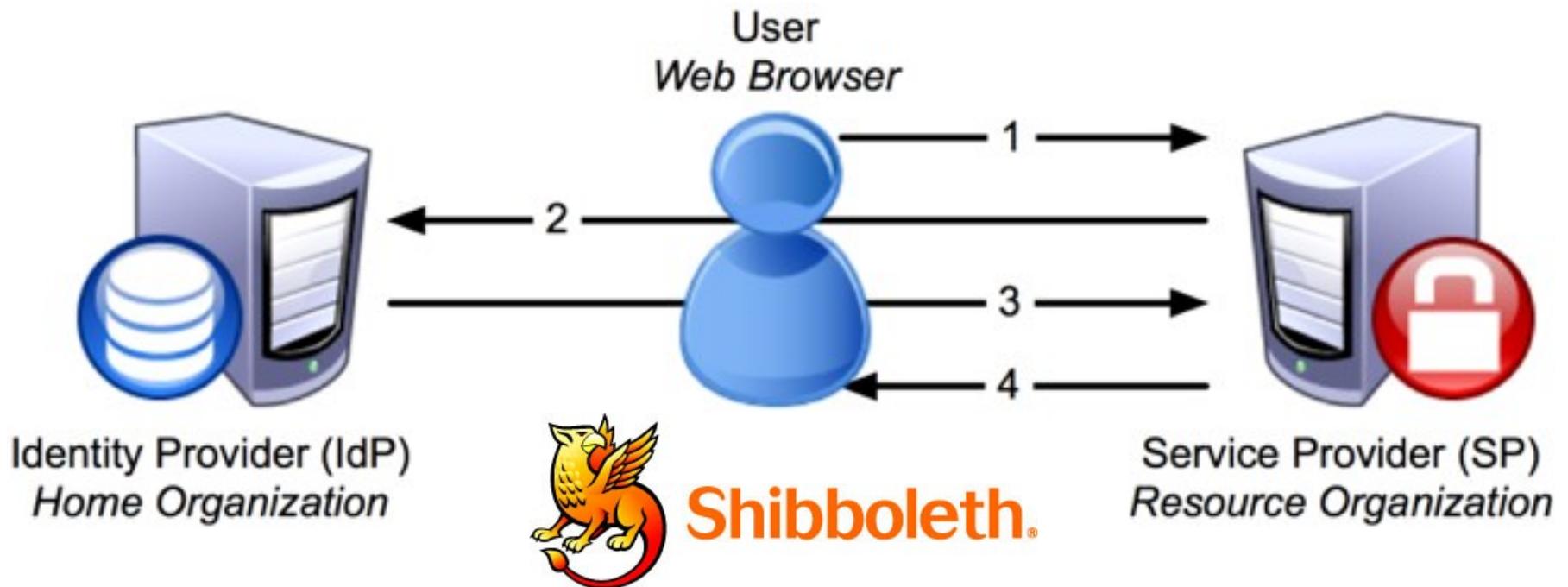
**Observatoire de Paris
VO-Paris Data Center**



Laboratoire Univers et Théories



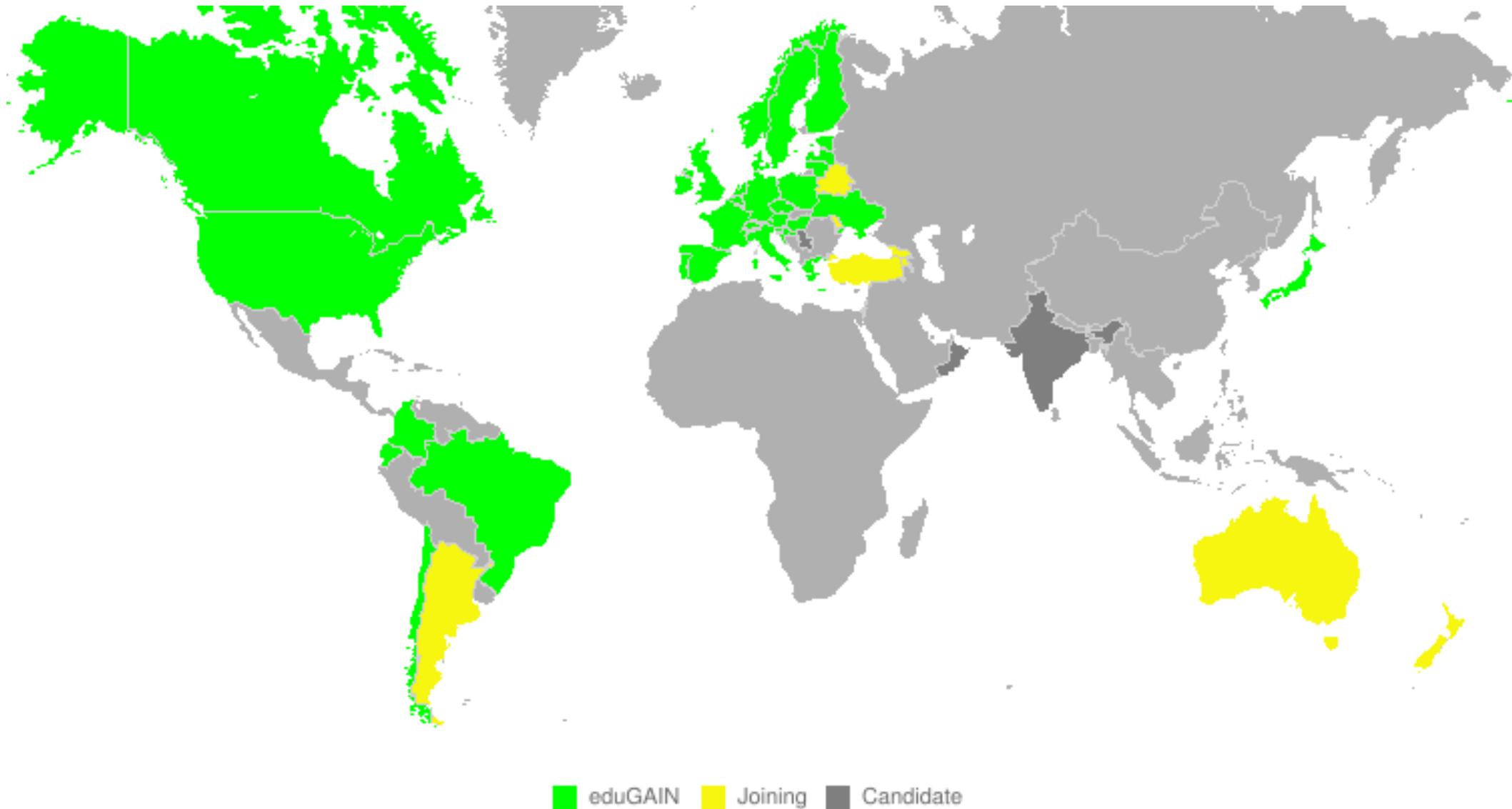
Single Sign-On with Identity Federations



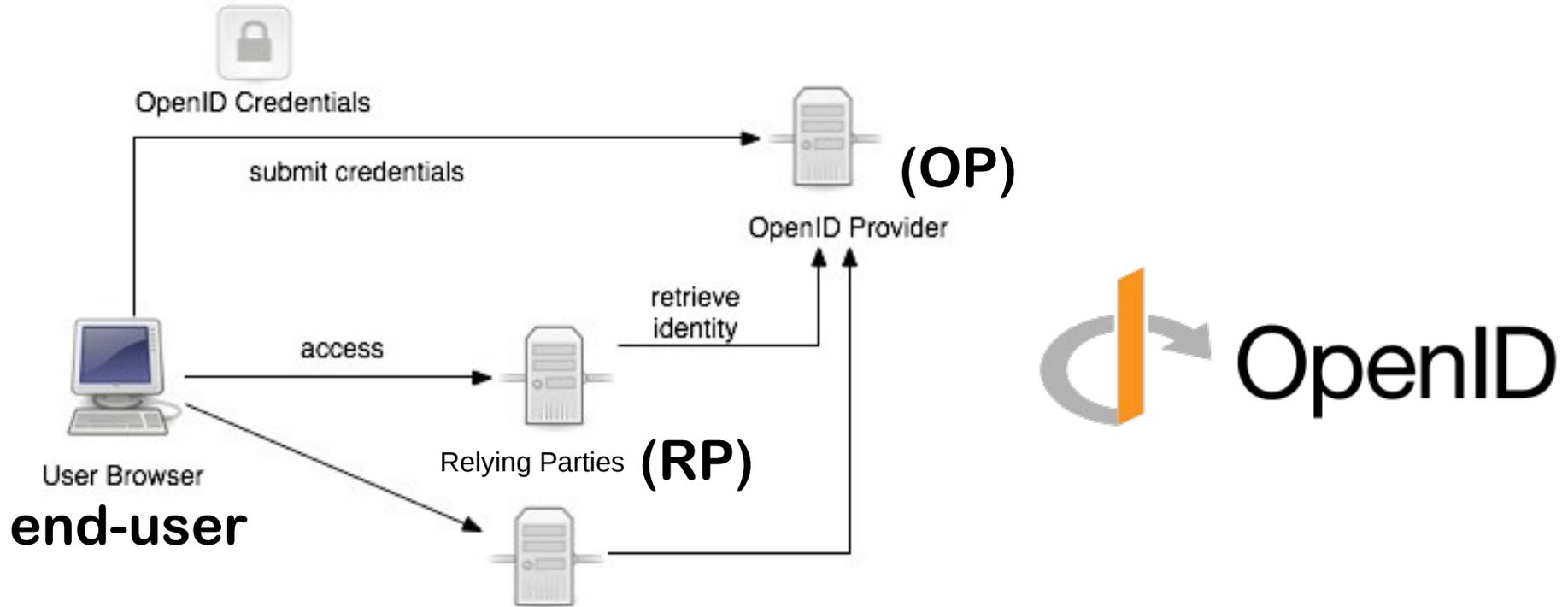
- ◆ **Shibboleth 2** = implementation of SAML2 for **SSO Authentication**
- ◆ **eduGAIN** : Identity Federation (RENATER, ...)
 - ◆ *Tested using Apache2 / mod_shib + mod_ssl + django-shibboleth-remoteuser*
 - ◆ **WAYF** (Where are You From) additional step to locate your IdP
 - ◆ Dedicated to **research community**
 - ◆ Dedicated to **web authentication**
 - ◆ Need to **register** the service in eduGAIN (with a x509 certificate)

eduGAIN status

<https://technical.edugain.org/status.php>



Social Networks: OAuth and OpenID

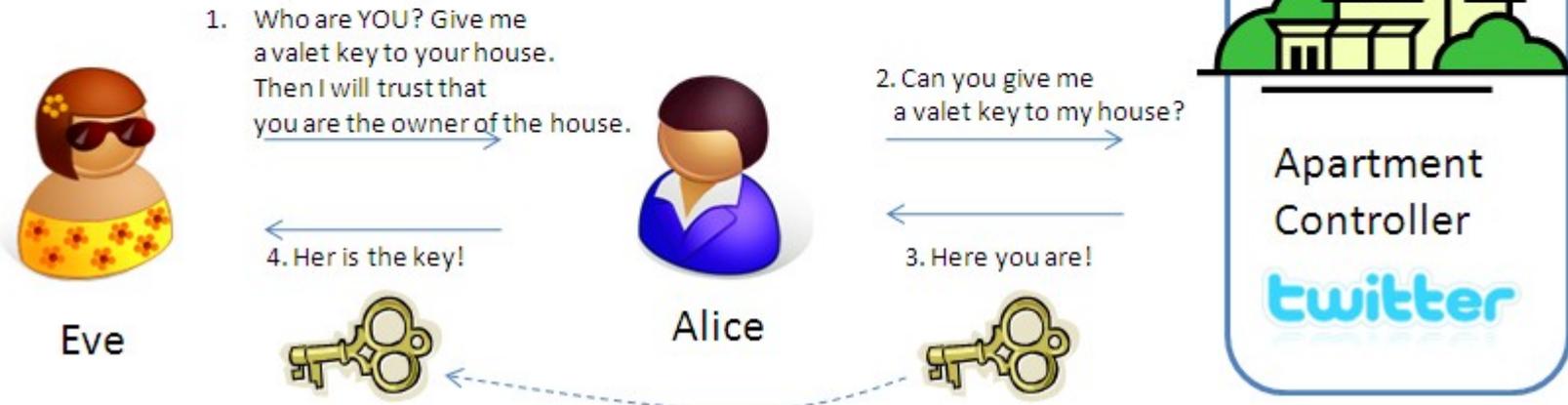


- ◆ **OpenID** is a way to use a single set of user credentials to access multiple sites
 - ◆ *Tested using Django + django-openid-auth*
- ◆ **OAuth 2** is an **authorization** framework usable for **authentication**
 - ◆ *Tested using Django + python-social-auth*
 - ◆ Need to **register** the service at OpenID Provider
- ◆ **OpenID Connect** (replacing OpenID) sits on top of the OAuth 2.0 framework
 - ◆ WebFinger : automatically finds your OP

OpenID vs OAuth

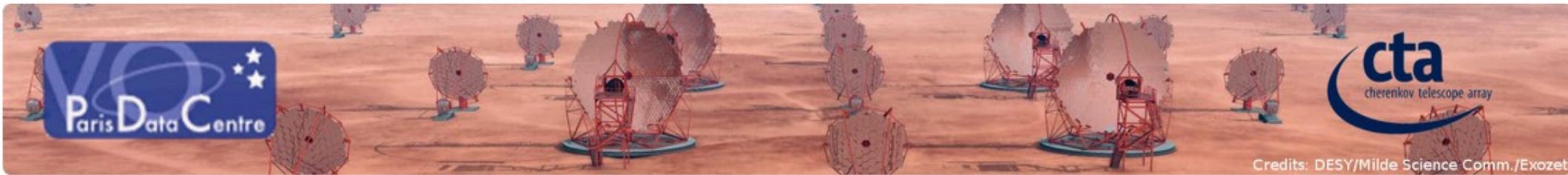


OAuth



Testing SSO for CTA Data Access

(Cherenkov Telescope Array)



CTA Data Distiller

🔍 Search Form

👤 Sign in

Sign in through eduGAIN

OR

OpenID:



OAuth:



OAuth2:



OR

Username

Password

Submit

Reset

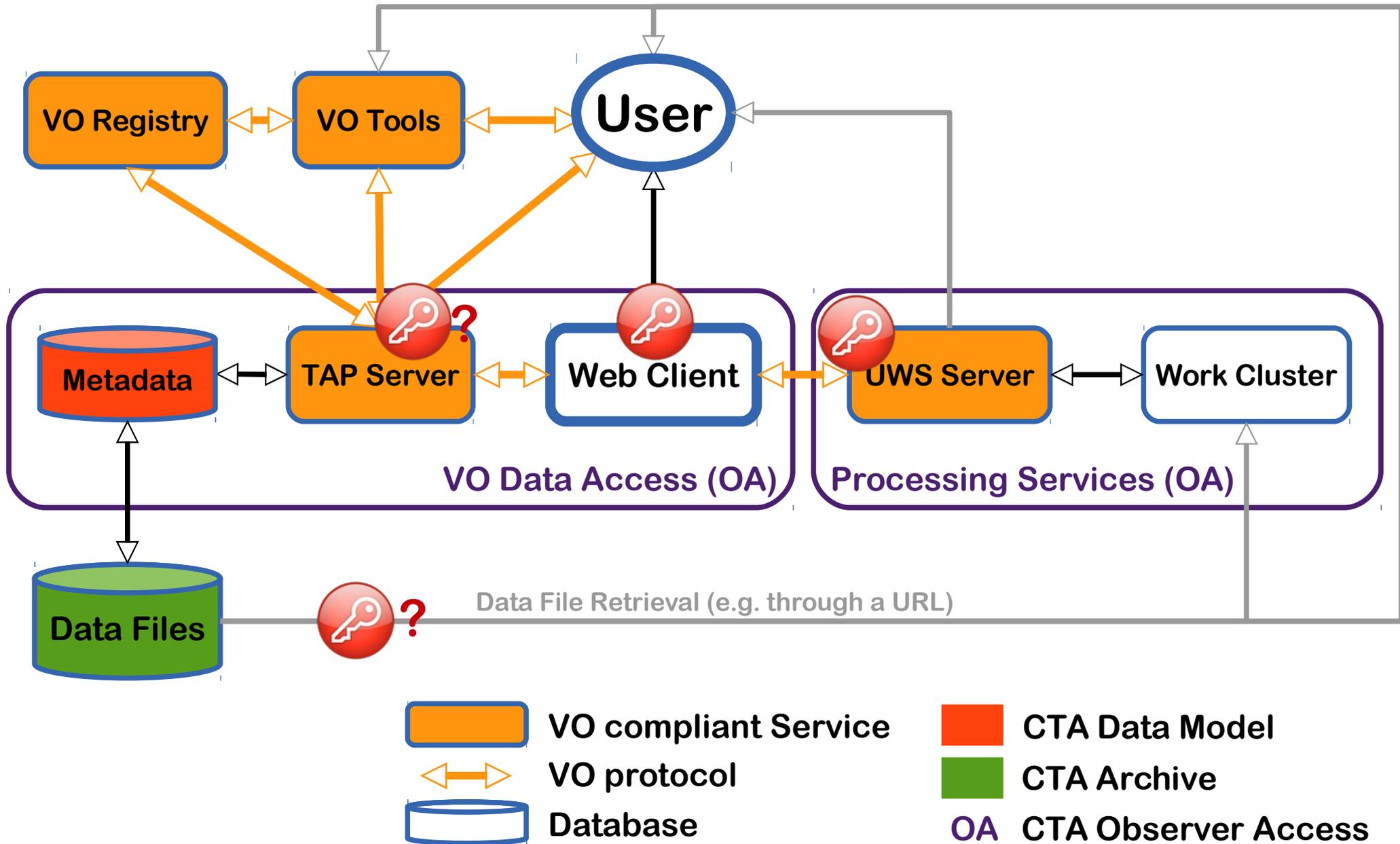
Main problems

- ◆ How to associate permissions to a user? (Authorization), OAuth, LDAP?
- ◆ How do I know that a user is in a specific ID federation? Is eduGAIN large enough?
- ◆ ID federation are usually associated to web authentication, how to use it with standalone application like Topcat / Aladin?

As a Service Provider

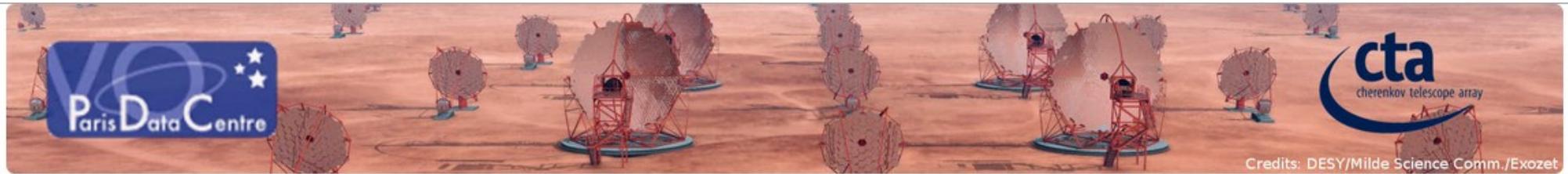
- ◆ How can I see that a user is a **VO user** and give him access to a resource? VO attributes?
- ◆ Do we want a centralised Database / Directory of VO user? Should we be Id Providers?
- ◆ Should I have a specific list of users including information of his authentication method (Shibboleth, OpenID, OAuth...)?

Use Case: Data Access for CTA



Web Client

<http://voparis-cta-client.obspm.fr>



CTA Data Distiller

Search Form

Job List

Sign out user

Cone Search

Target Name

Crab Nebula

Used to query Simbad with Sesame and set RA/Dec.

Source RA (deg)

83.633

Source Dec (deg)

22.514

Search radius (deg)

0.001

Submit

Reset

- ◆ Django, jQuery, Bootstrap3
- ◆ Name resolver
- ◆ Simbad through Sesame
- ◆ Builds and Sends the ADQL query

ObsCore Search

proposal_id

Proposal ID

dataprodect_type

Nothing selected

Data product (file content) primary type

dataprodect_level

Nothing selected

DL0-5

Search

Analyse

Visualisation

SAMP

Interop (SAMP)

Send Result Table

Send Selected Data

Analysis tools

Create Count Map(s)

Extract Spectrum

Plotting tools

TOPCAT

Aladin

VOSpec

SPLAT

Results

```
SELECT * FROM cta.vo_obscore as o WHERE 1 = intersects(o.s_region, circle('ICRS', 83.63308333, 22.0145, 0.001))
```

Send

ADQL query

ObsCore fields

Search

UWS

	dataprodct_type	obs_collection	obs_id	target_name	s_ra (deg)	s_dec (deg)
<input type="checkbox"/>	eventlist	1	23592	Crab Nebula	82.01333618164062	22.01444435119629
<input type="checkbox"/>	eventlist	1	23559	Crab Nebula	85.25333404541016	22.01444435119629
<input type="checkbox"/>	eventlist	1	23526	Crab Nebula	83.63333129882812	22.51444435119629
<input type="checkbox"/>	eventlist	1	23523	Crab Nebula	83.63333129882812	21.51444435119629
<input type="checkbox"/>	eventlist	3	5003499	CrabNebula	83.28087615966797	21.784133911132812

Showing 1 to 5 of 10 rows records per page

<< < 1 2 > >>