Authentication & Authorization systems developed for CTA

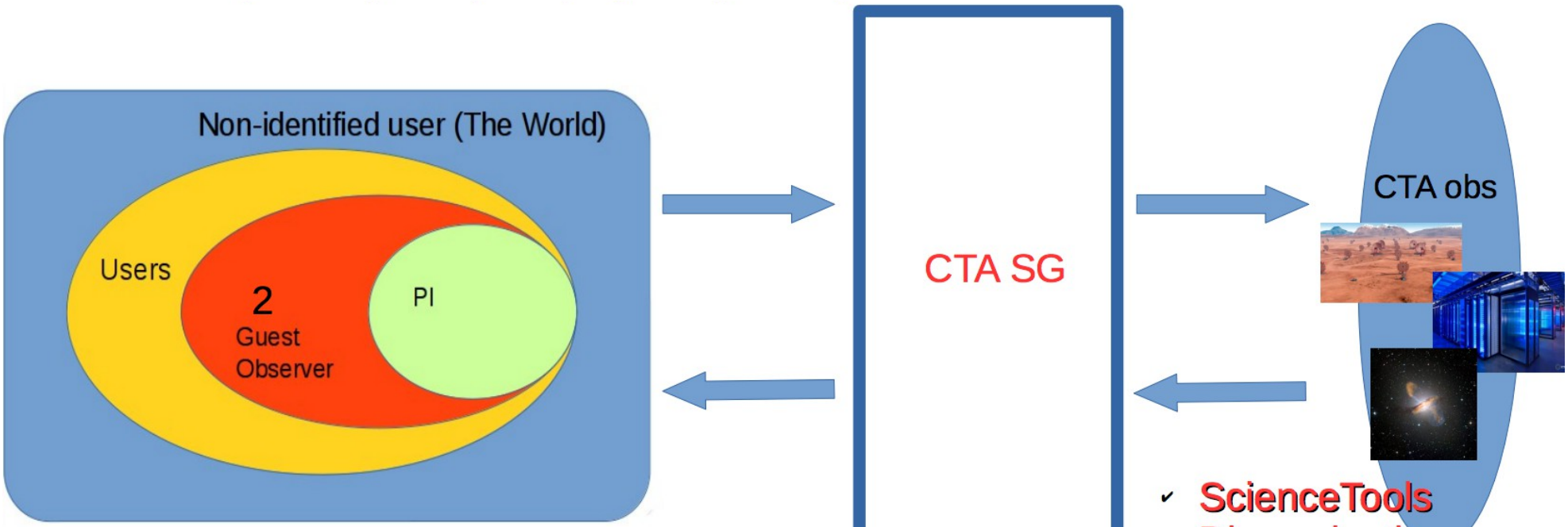
Mathieu Servillat

Observatoire de Paris
Paris Astronomical Data Centre

ASTERICS DADI Second Tech Forum in Edinburgh

Context: the CTA Science Gateway

The contact point for the world to CTA



- Info/tuto
- Data
- Observations
- ...

- ScienceTools
- Dissemination
- Pipeline
- Archive
- Proposal Handling
- Control of the Array
- ...

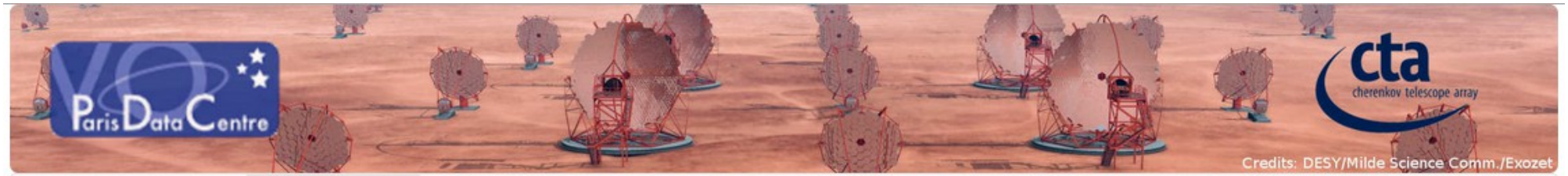
@ David Sanchez, LAPP

CTA Gateway working group

Catherine Boisson; Alessandro Costa; Bruno Khelifi; Eva Sciacca; Giovanni Lamanna; Piero Massimino; Nadine Neyroud; David Sanchez; Mathieu Servillat; Hubert Siejkowski; Tomasz Szepieniec and Joanna Kocot

@ David Sanchez, LAPP

CTA Data Distiller 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	

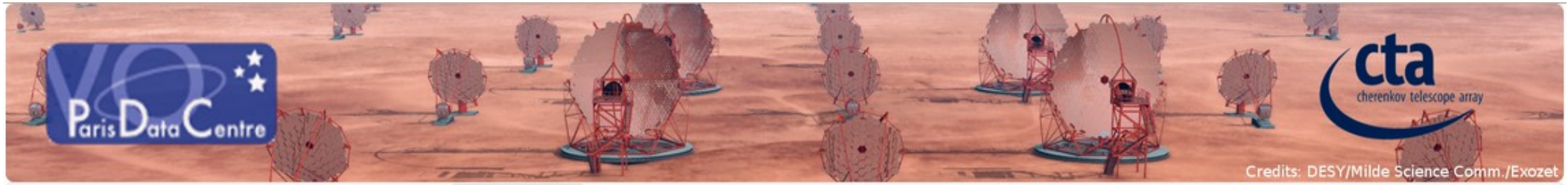
Submit Reset

- Django, jQuery, BootStrap3
- Name resolver
  Simbad through Sesame
- Builds and Sends the ADQL query

ObsCore Search

proposal_id		Proposal ID
dataproduct_type	Nothing selected	Data product (file content) primary type
dataproduct_level	Nothing selected	DL0-5

CTA Data Distiller http://voparis-cta-client.obspm.fr



CTA Data Distiller | Search Datasets | Results | Job List | Selected Job | JS9 | Authentication: Sign out **user**

Search | Analyse | Visualisation

SAMP

Interop (SAMP)

Send Result Table

Results

show/hide query

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

Analysis tools

Create Count Map(s)

	dataproduct_type	obs_collection	obs_id	target_name	s_ra (deg)	s_dec (deg)
☐	eventlist	1	23592	Crab Nebula	82.01333618164062	22.01444435119629
☐	eventlist	1	23559	Crab Nebula	85.25333404541016	22.01444435119629
☐	eventlist	1	23526	Crab Nebula	83.63333129882812	22.51444435119629
☐	eventlist	1	23523	Crab Nebula	83.63333129882812	21.51444435119629
☐	eventlist	3	5003499	CrabNebula	83.28087615966797	21.784133911132812

Showing 1 to 5 of 10 rows 5 records per page

<< < 1 2 > >>

Plotting tools

TOPCAT

Aladin

VOSpec

SPLAT

Gateway meetings

- Last meeting in Meudon (Dec. 2015)
- Open session for ASTERICS members
- Technology choices
- Prototypes

Open session: (through Renater Rendez-Vous,

09:20 **CTA Gateway work package** *20'*
Speaker: Dr. David Sanchez (LAPP)
Material: **Transparents**

09:40 **Requirements and Use Cases** *20'*
Speaker: Mrs. Nadine Neyroud (LAPP/IN2P3/CN
Material: **Slides**

10:00 **Current prototype status and Unity IDM** *2*
* *Top menu bar*
* *Message bus*
* *A&A*

Speakers: Dr. Hubert Siejkowski (ACC Cyfronet
Joanna Kocot (ACC Cyfronet AGH)
Material: **Slides** **text**

10:20 **Grouper/Shibboleth prototype** *20'*
Speaker: Dr. Alessandro Costa (INAF)
Material: **Slides**

11:00 **SKA A&A system (ASTERICS project conn**
by Cristina Knapic
Material: **Transparents**

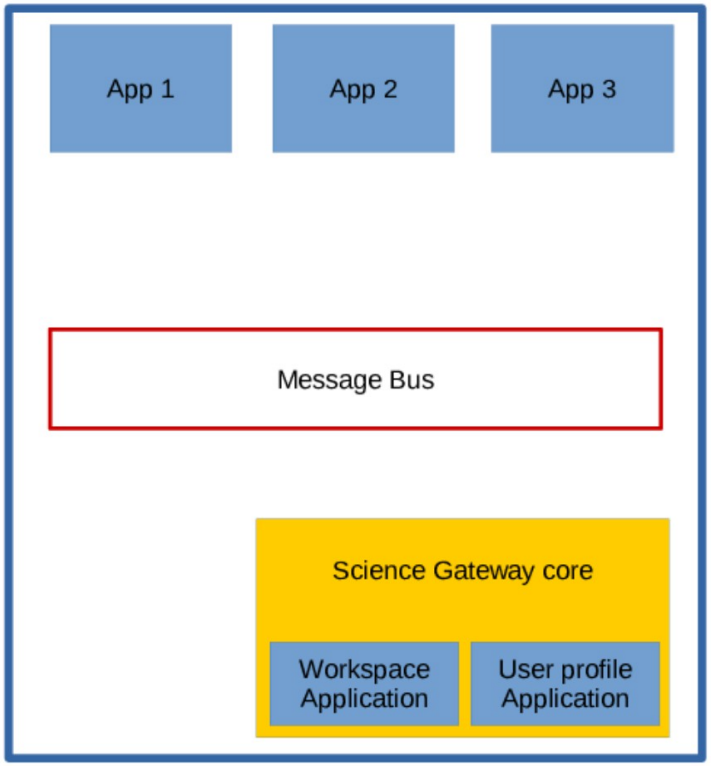
11:20 **A&A in the Virtual Observatory (ASTERIC**
by Marco Molinaro
Material: **Transparents**

11:40 **Discussions** *50'*

Gateway common integration rules

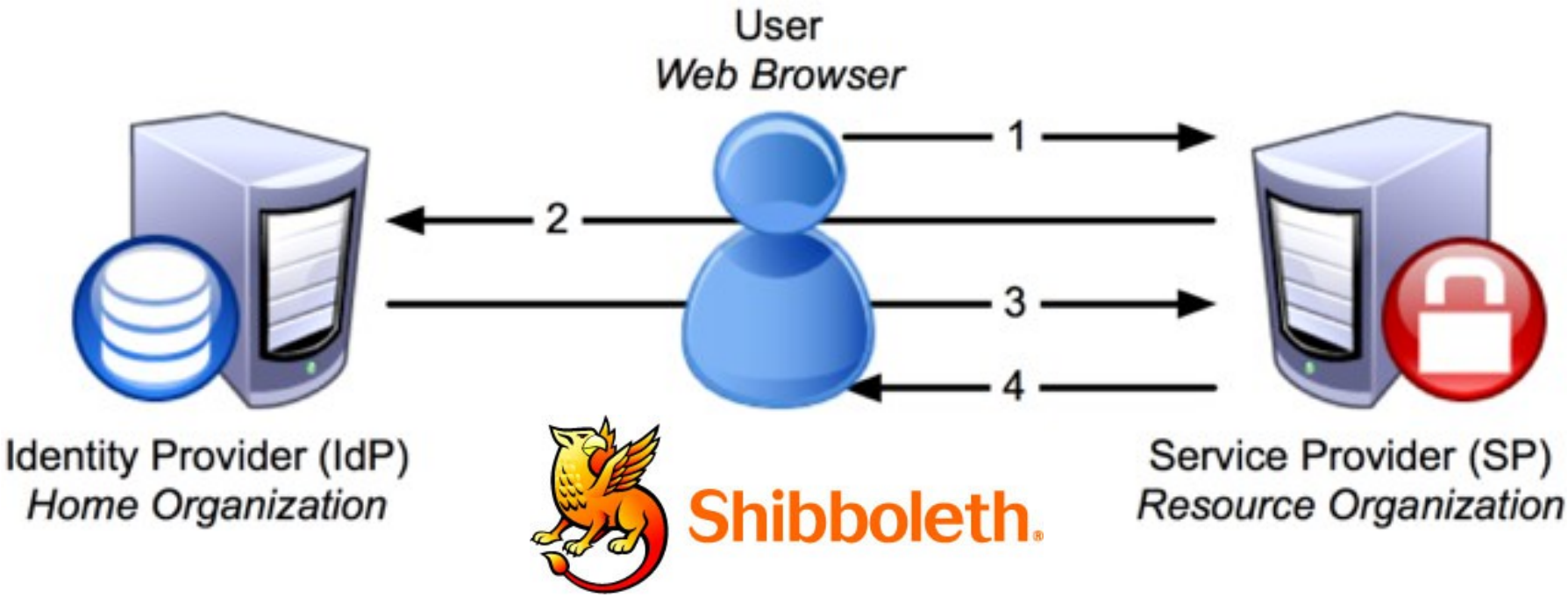
- **Top Menu Bar** for all applications
  - A common HTML code should appear on all Gateway services, accessible through e.g. a single URL or using proxys
  - A common style: Bootstrap3 fixed navbar, which is the library already used by the Distiller
  - *Tested for the Data Distiller*:

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



- A common **message bus**
  - RabbitMQ + ProtoBuf
- **Centralized A&A prototypes**
  - Unity
    http://www.unity-idm.eu/
  - Grouper
    http://www.internet2.edu/products-services/trust-identity-middleware/grouper/
  - *Being tested with Django plugins*

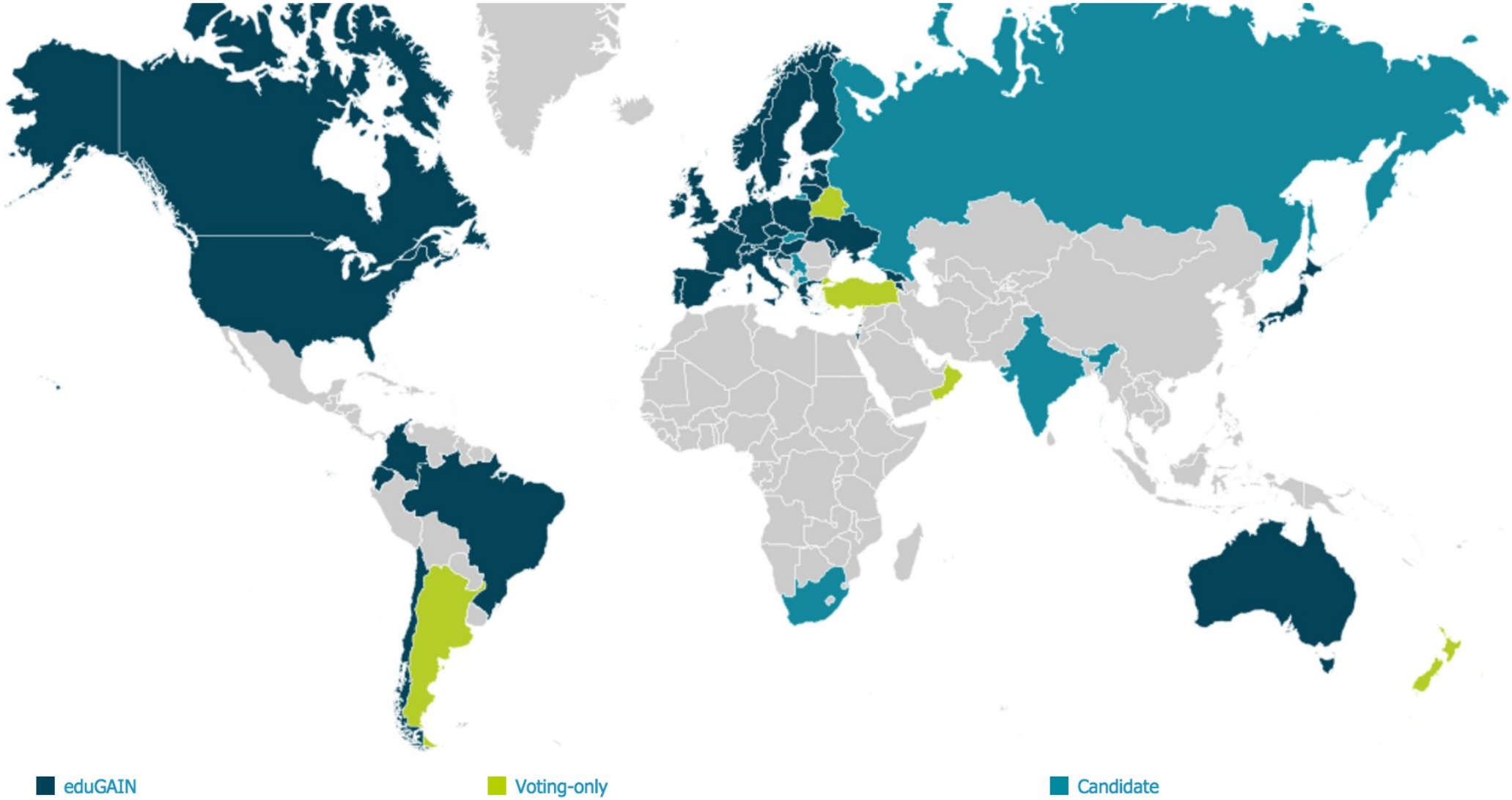
Single Sign-On with Identity Federations



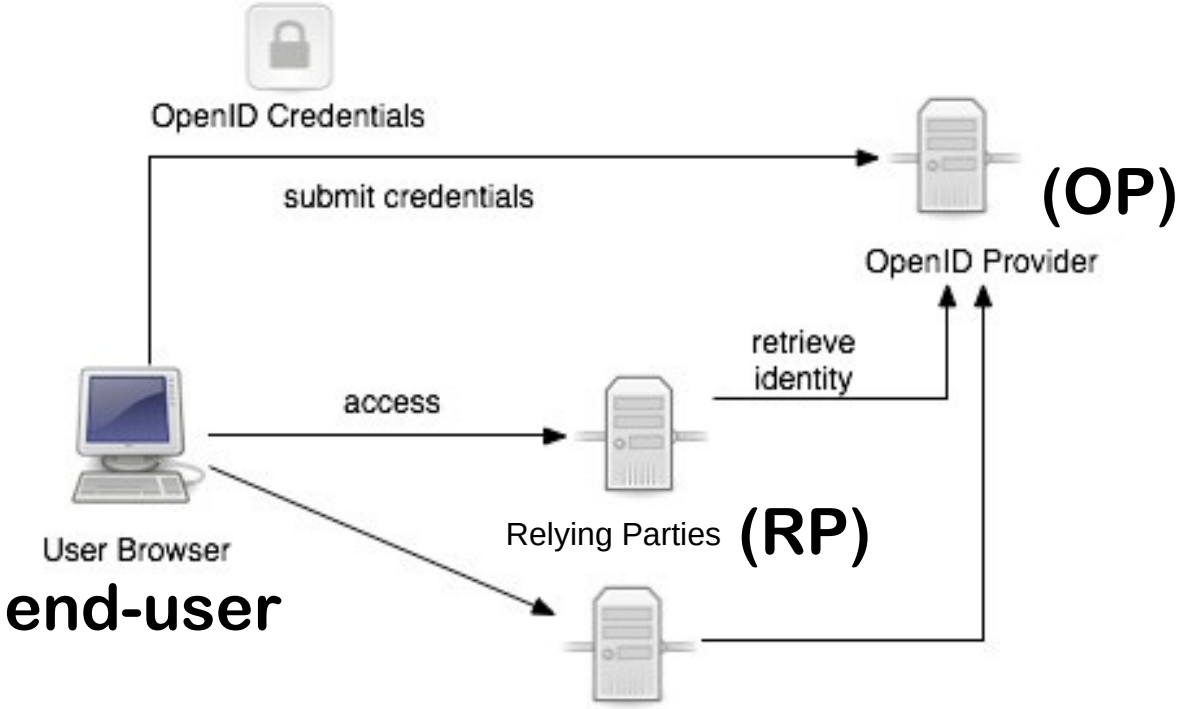
- Shibboleth 2 = implementation of SAML2 for **SSO Authentication**
- eduGAIN : Identity Federation (RENATER, …)
  - *Tested using Apache2 / mod_shib + mod_ssl + django-shibboleth-remoteuser*
  - Dedicated to research community
  - Dedicated to **web** authentication
  - WAYF (Where Are You From): additional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

eduGAIN status

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



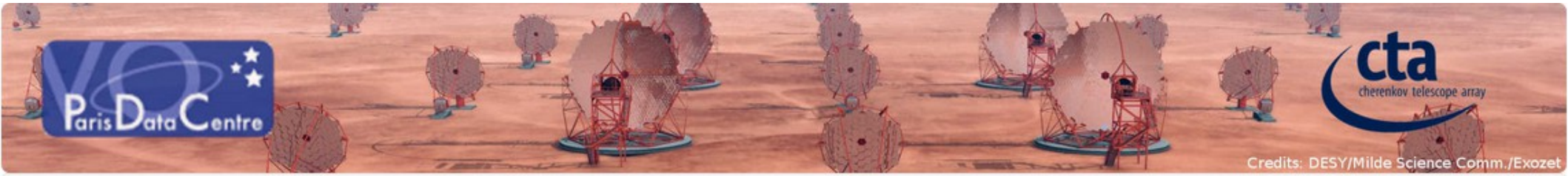
Social Networks: OAuth and OpenID



- 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 OP
- OpenID Connect (now replacing OpenID) sits on top of the OAuth 2.0 framework
  - WebFinger : automatically finds your OP

Testing SSO for CTA VO Data Access

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



CTA Data Distiller Search Form Sign in

Sign in through eduGAIN

OR

OpenID: OAuth: OAuth2:

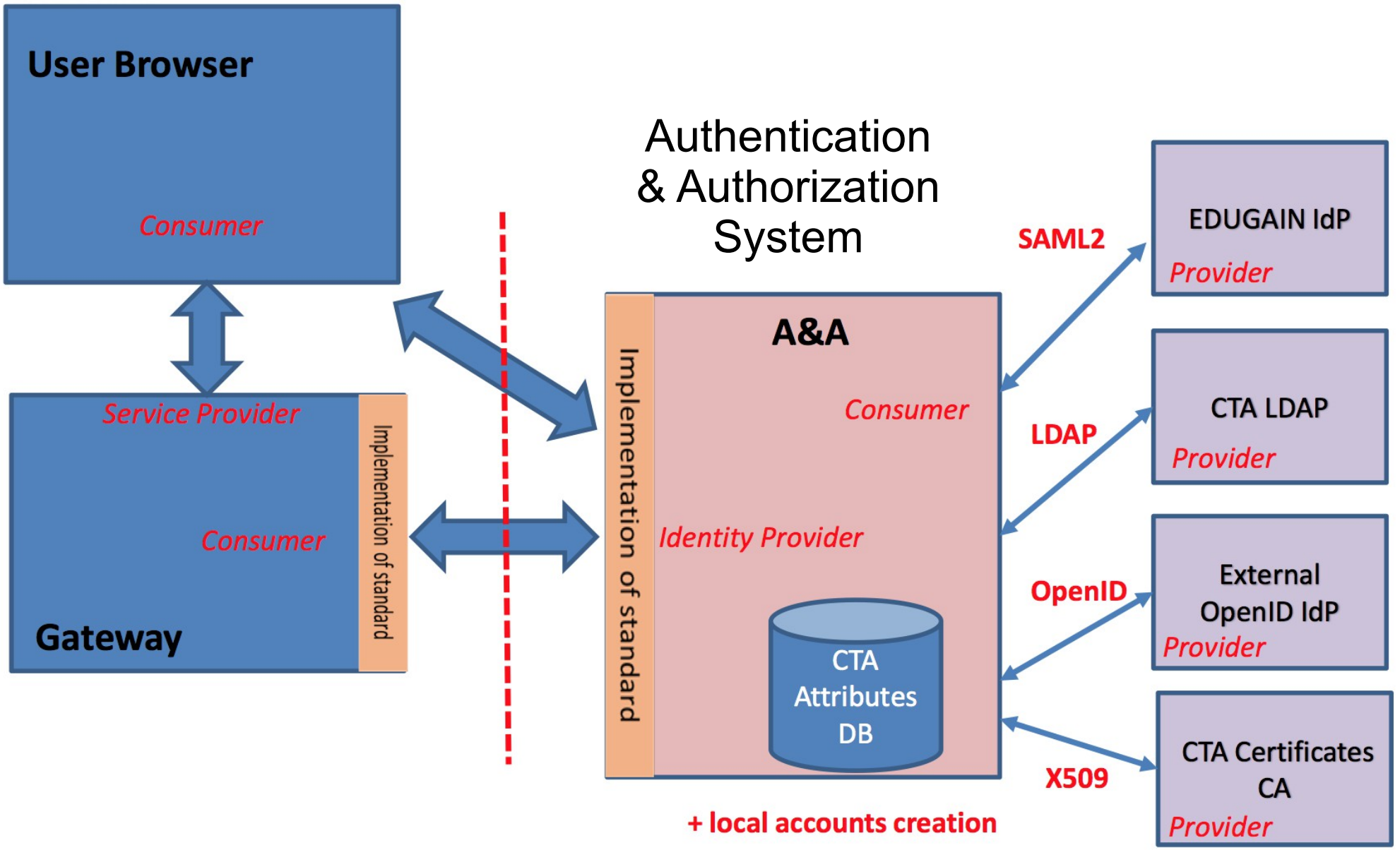
OR

Username: user

Password: •••

Submit Reset

CTA Science Gateway A&A

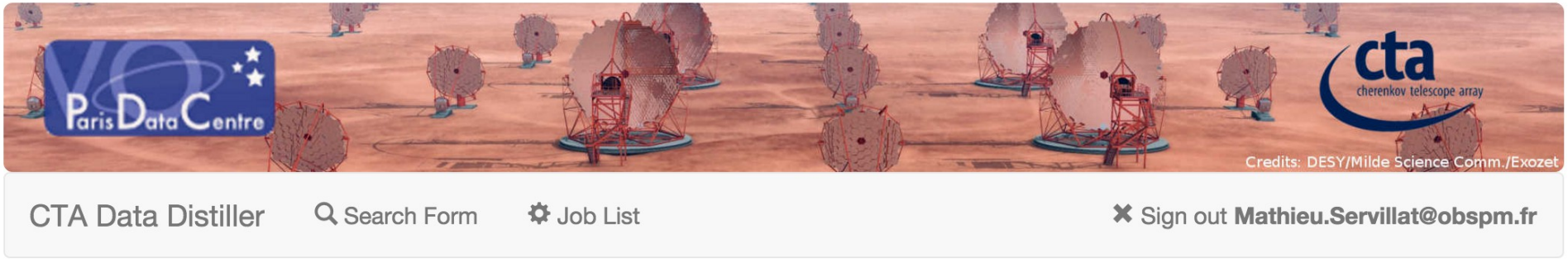


A&A with Grouper

- Grouper is an access management system, used to create and manage institutional and personal groups, roles and permissions
- Developped by internet2 (US research and education network)
- Open-source software (Apache 2.0 licence)
- Same « spirit » as for eduGAIN and Shibboleth
- Widely used for research and education (LIGO, LHC...)

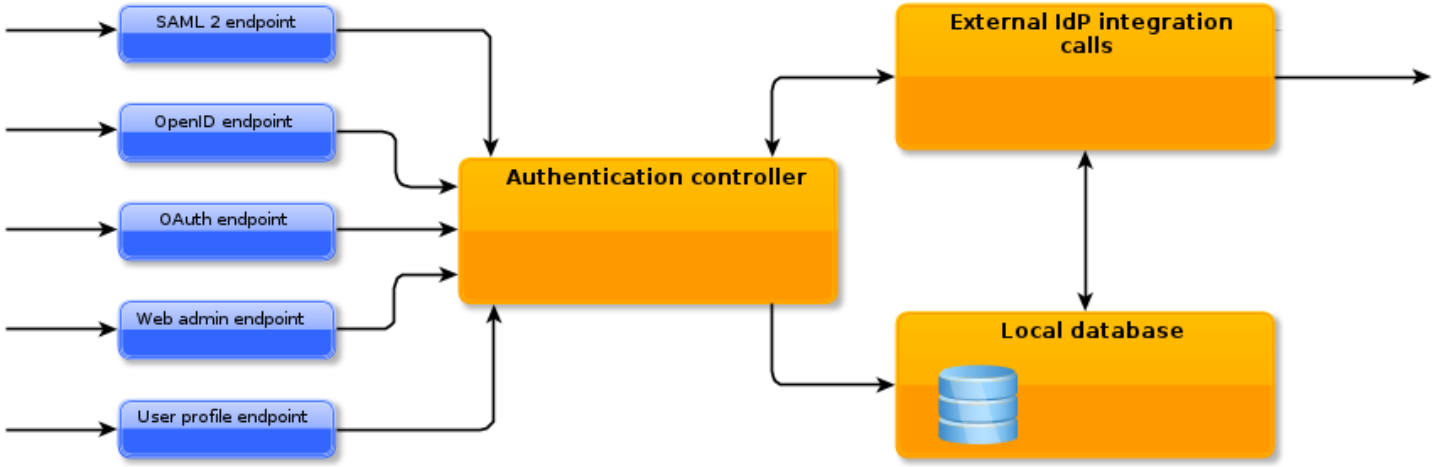
Grouper prototype at INAF

- Authentication with Shibboleth
- List of attributes from Grouper service at INAF



A&A with Unity

- Solution for identity, federation and inter-federation management
- Lead by ICM (University of Warsaw)
- based on UVOS experience (UNICORE Virtual Organisations System)
- Open Source (permissive BSD licence)



Unity core concepts

- Cloud approach: **Identity Management As a Service** with attributes management and authentication included.
- **Multiple authentication protocols** supported
  - SAML2, OpenID Connect, LDAP...
- Ability to **outsource** credentials (and attributes) management to a 3rd party service.
  - Again multiple upstream protocols supported
  - UNITY becomes a **bridge** (protocol translation)...
  - ... and a **hub** (single service aggregating various IdM systems).

- **Persistent ID** connecting to several accounts
- Attached **attributes** to compute user rights inside apps

Conclusions

- Both A&A systems provide:
  - authentication through federations (no need to manage user affiliations and passwords)
  - local management of user attributes and rights (specific to the project, so cannot be delegated)
  - Simple interface to manage the system
- Unity is not restricted to the eduGAIN federation
  - Handles OpenID, certificates, LDAP…
- Connections to the VO:
  - SAMP blocked over HTTPS (mixed content blocked)
  - TAP or UWS with authentication/SSO?