Authentication & Authorization systems developed for CTA

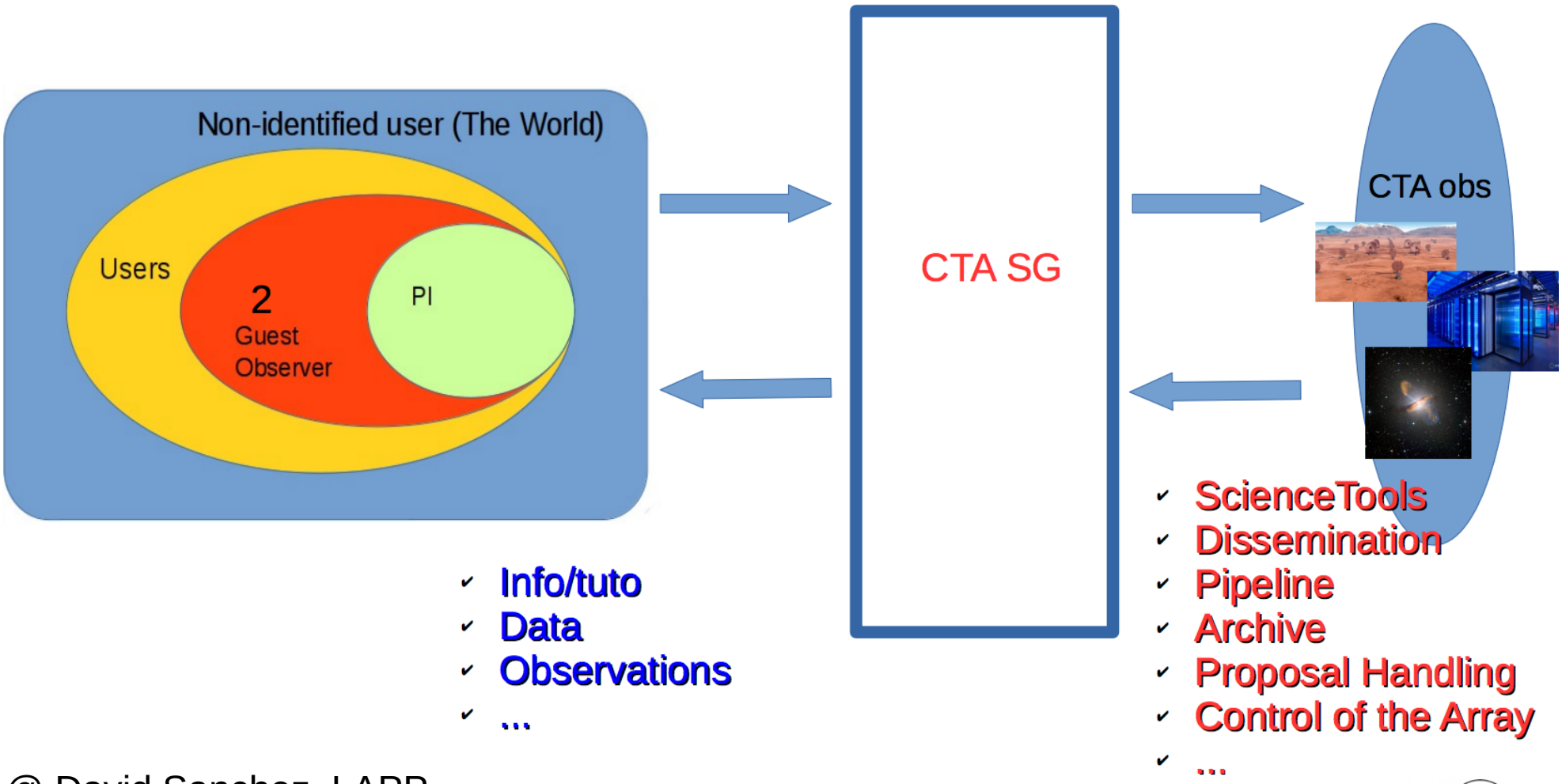
Mathieu Servillat

Observatoire de Paris
Paris Astronomical Data Centre

IVOA Cape Town meeting

Context: the CTA Science Gateway

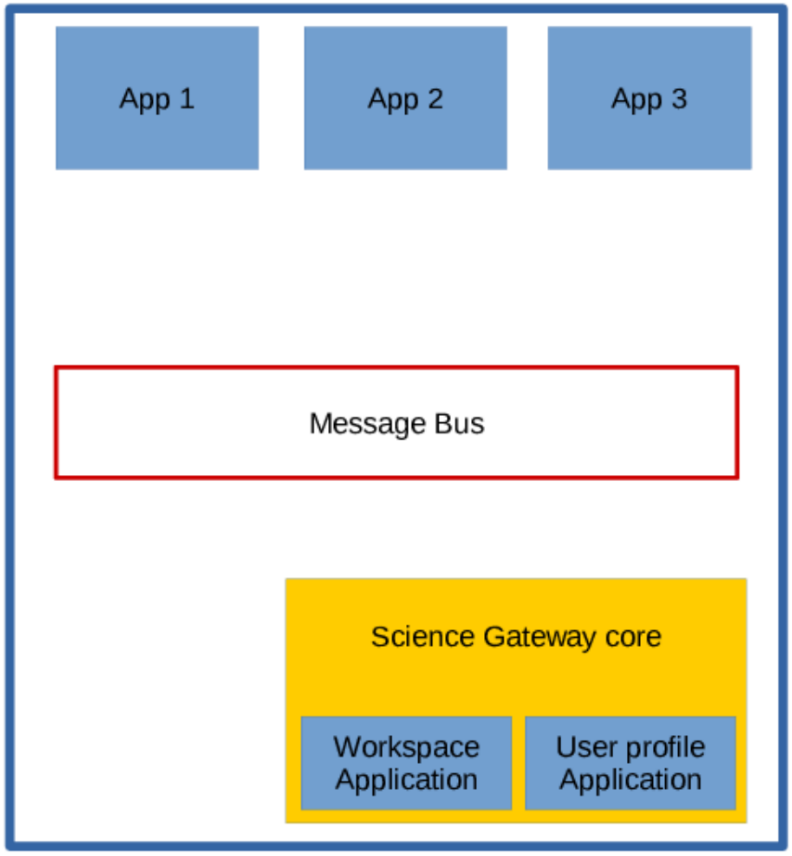
The contact point for the world to CTA



@ David Sanchez, LAPP

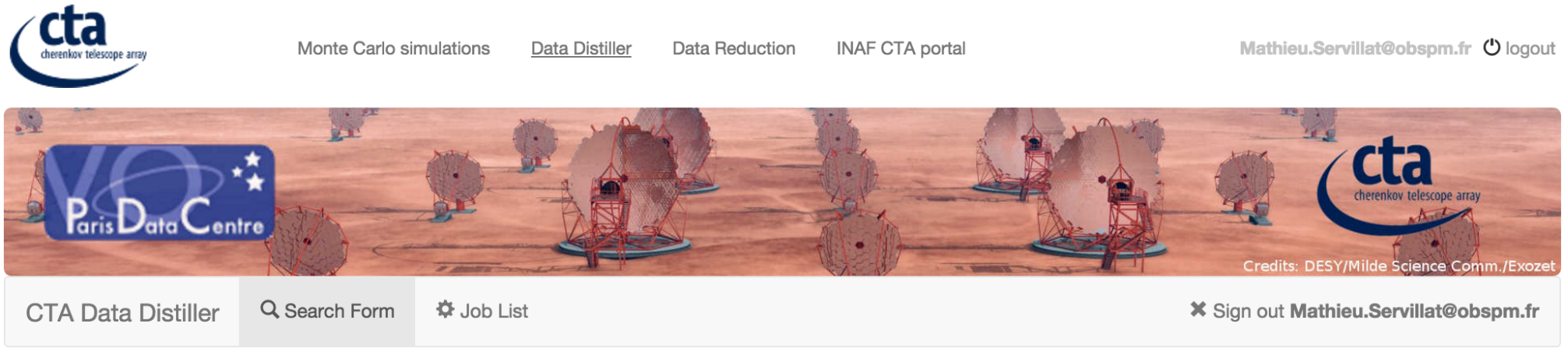
Gateway common integration rules

- **Top Menu Bar** for all applications
  - A common HTML code on all Gateway services, accessible through e.g. a single URL or using proxys
  - A common style: Bootstrap3
- A common **message bus**
  - RabbitMQ + ProtoBuf
- **Centralized A&A prototypes**
  - Grouper and Shibboleth
    http://www.internet2.edu/products-services/trust-identity-middleware/grouper/
  - Unity Identity Manager
    http://www.unity-idm.eu/



CTA Data Distiller

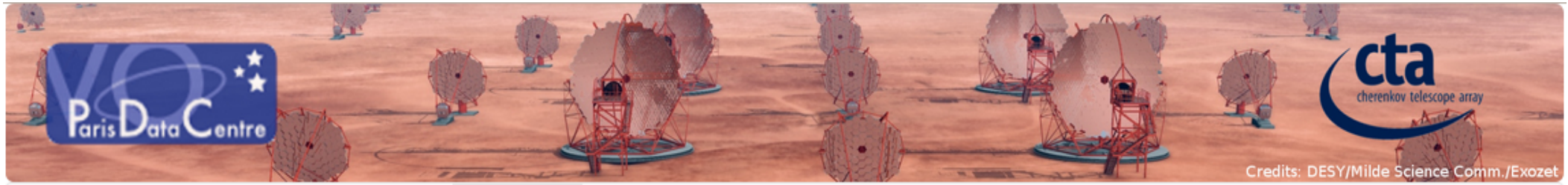
https://voparis-cta-test.obspm.fr



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

CTA Data Distiller

https://voparis-cta-test.obspm.fr



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

Search | Analyse | Visualisation

SAMP

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))

ADQL query

Send

ObsCore fields

Search

UWS

	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 > >>

Interop (SAMP)

Send Result Table

Analysis tools

Create Count Map(s)

Plotting tools

TOPCAT

Aladin

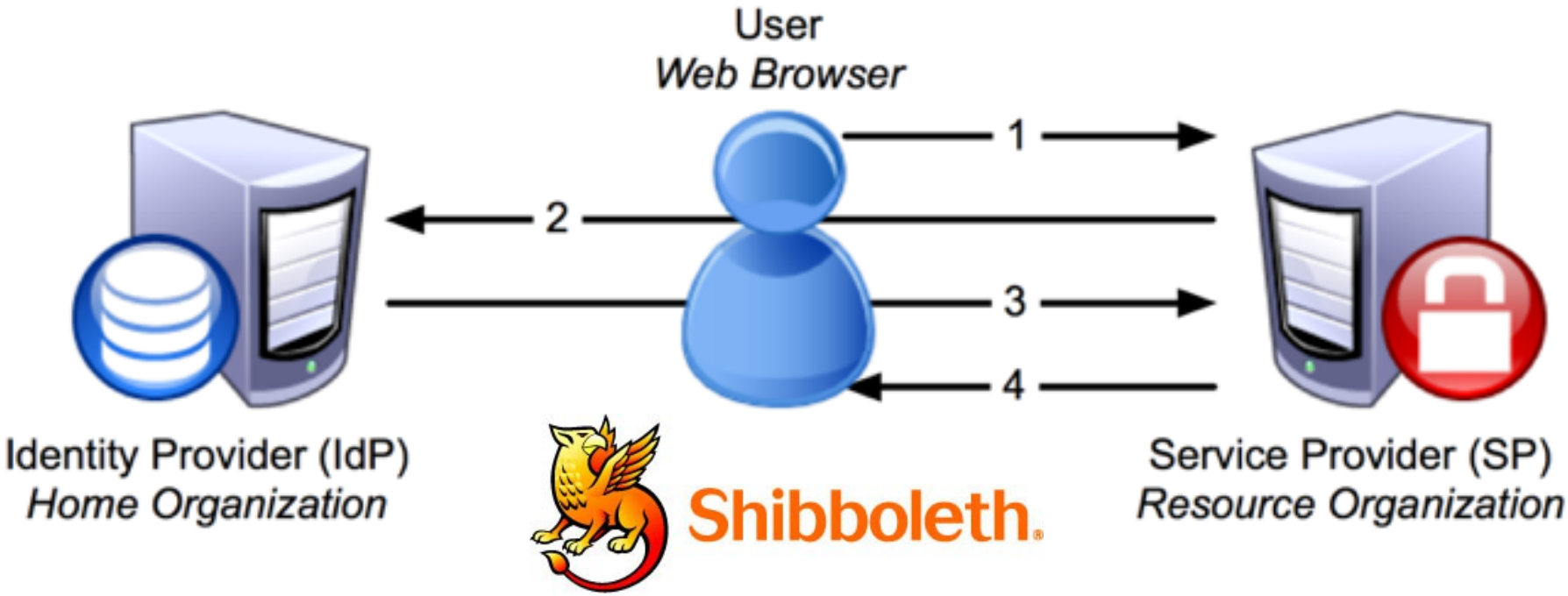
VOSpec

SPLAT

Testing SSO in the CTA Data Distiller

- Shibboleth+Grouper
  - EduGAIN federation
  - SAML2
- Unity IDM
  - Uses OpenID Connect
- OpenID Connect
  - Google as an IdP
- OAuth2
  - Github, Google, Facebook, ...
- OAuth
  - Twitter, ...
- OpenID 2.0 (deprecated)
- Local account

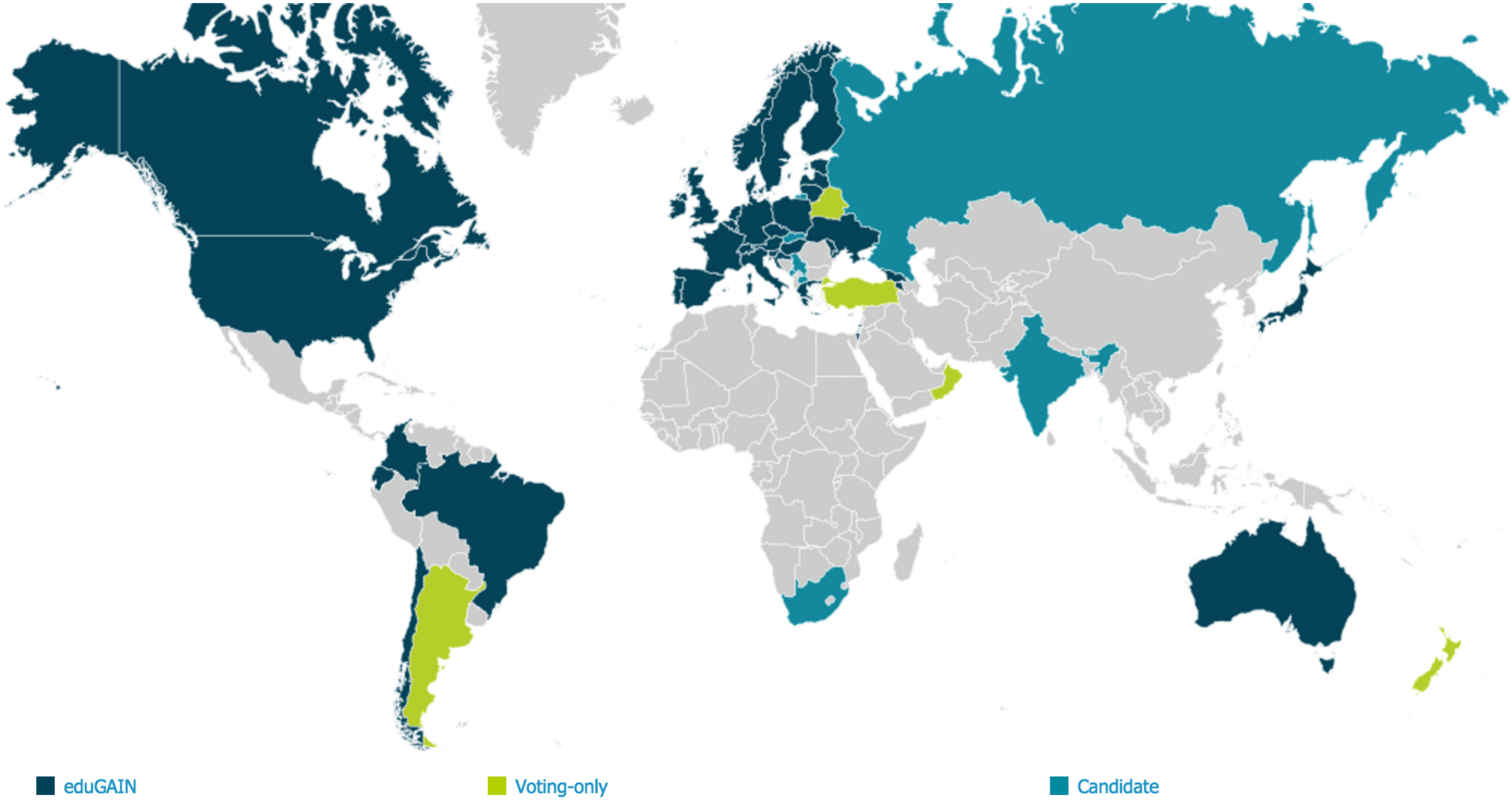
Single Sign-On with Identity Federations



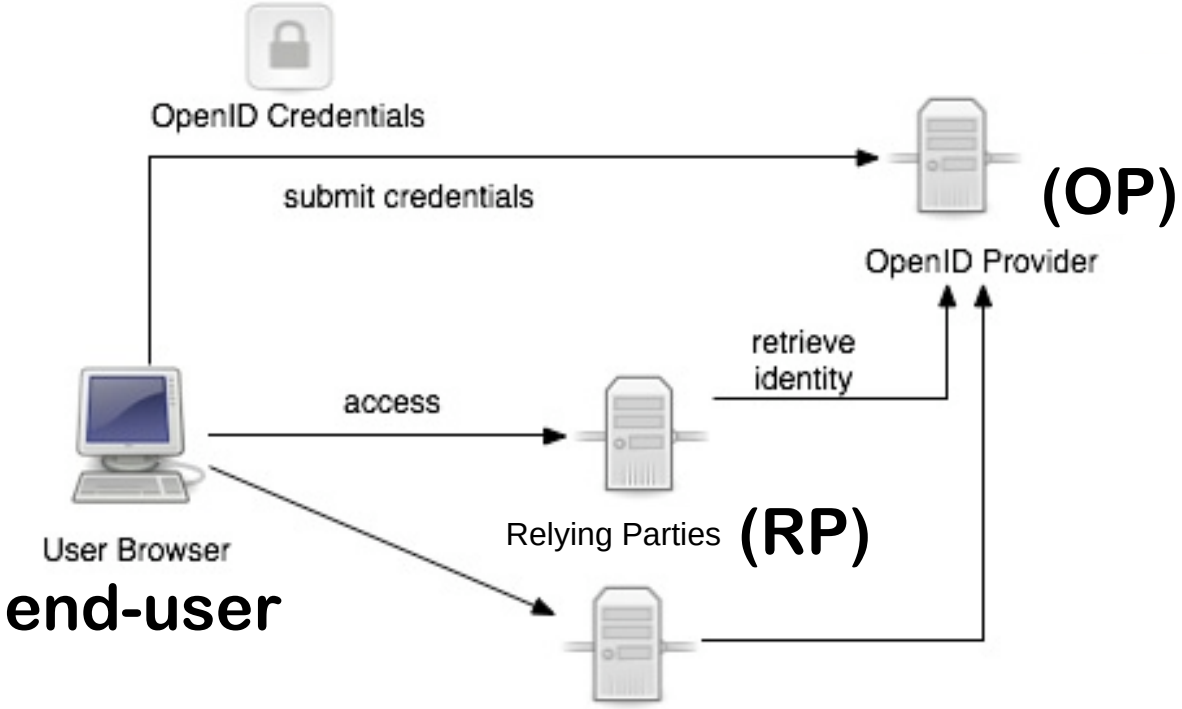
- Shibboleth2 = SAML2 for **SSO Authentication**
- eduGAIN : Identity Federation (RENATER, …)
  - Dedicated to research community
  - Dedicated to **web** authentication
  - WAYF (Where Are You From): additional step to locate your IdP

eduGAIN status

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



Social Networks: OAuth and OpenID



- OAuth2: **authorization** framework usable for **authentication**
- OpenID is a way to use a single set of user credentials to access multiple sites
- OpenID Connect, on top of the OAuth 2.0 framework
  - WebFinger : automatically finds your OP

A&A with Grouper

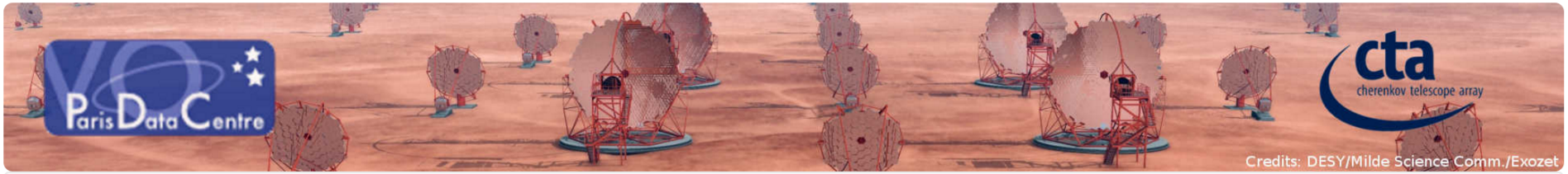
- Grouper is an access management system, used to create and manage institutional and personal groups, roles and permissions
- Developed by internet2 (US research and education network)
- Open-source software (Apache 2.0 licence)
- Same « spirit » as for eduGAIN and Shibboleth
- Widely used for research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

Shibboleth/Grouper configuration

- Install mod_shib module for Apache
- Register Service on eduGAIN (through RENATER)
  https://services.renater.fr/federation/docs/fiches/sp_edugain_enabled
  - Generate x509 cetificate
  - Set shibboleth2.xml file
  - Set attribute-map.xml
  - Inscription to test federation, then eduGAIN
- Link to Grouper server (prototype at INAF)
  - Copy Attribute Authority Metadata
    /etc/shibboleth/CTA-grouper-metadata.xml
  - Modify shibboleth2.xml file
    <MetadataProvider type="XML" path="/etc/shibboleth/CTA-grouper-metadata.xml "/>
  - Edit attribute-map.xml
  - Edit attribute-policy.xml

Shibboleth/Grouper prototype

- Authentication with Shibboleth (find IdP, enter login/password)
- Get list of attributes from Grouper (using EPPN attribute)

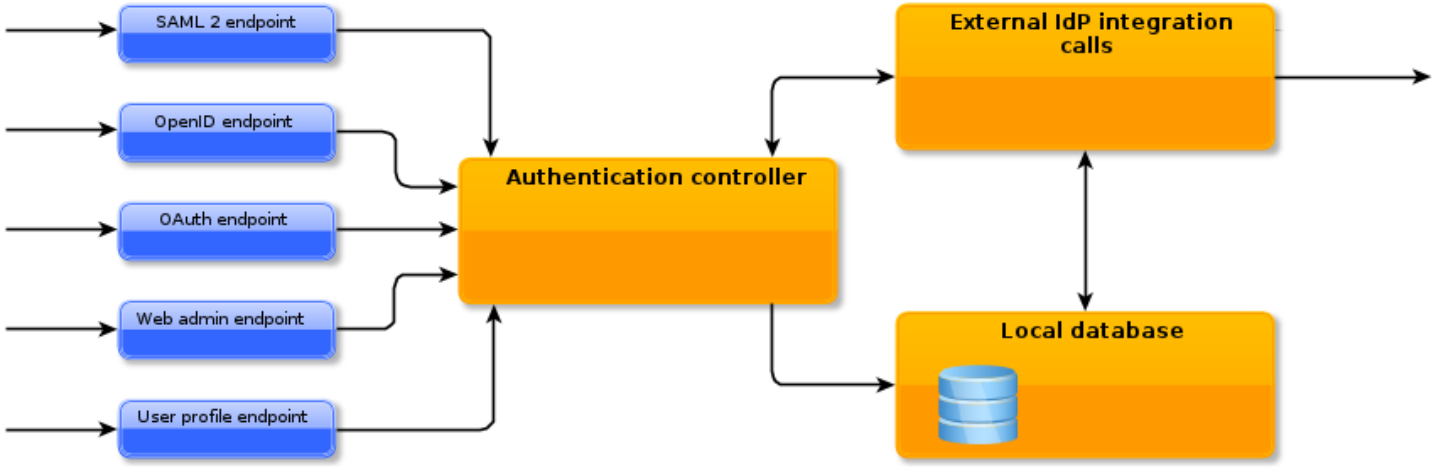


CTA Data Distiller | Search Form | Job List | Sign out **Mathieu.Servillat@obspm.fr**

```
HTTP_DISPLAYNAME = Mathieu Servillat
HTTP_ENTITLEMENT = urn:mace:garr.it:voparis-auth.obspm.fr;urn:mace:dir:entitlement:common-lib-terms
HTTP_EPPN = mservillat@obspm.fr
HTTP_FACSIMILETELEPHONENUMBER =
HTTP_GIVENNAME = Mathieu
HTTP_HOST = voparis-cta-client.obspm.fr
HTTP_ISMEMBEROF = AdvancedWFUser
HTTP_L = Meudon
HTTP_MAIL = Mathieu.Servillat@obspm.fr
HTTP_NICKNAME =
HTTP_O =
HTTP_ORGUNIT_DN =
HTTP_ORG_DN =
HTTP_OU =
HTTP_PERSISTENT_ID = https://shibboleth.obspm.fr/idp/shibboleth!https://voparis-auth.obspm.fr/!oSJ+0RqfJvuv0Yos8S8MbGM/To8=
HTTP_POSTALADDRESS =
HTTP_POSTALCODE =
```

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

Unity configuration and sequence

- Register service at OpenID IdP
  - Get **id** and **key**
  - Set **redirect** URIs (callbacks)
- Configure OpenID Connect client
  - Django OIDC package
  - Set Unity **server URL**

- Send OpenID request to Unity server (with **id** and **state**)
- Log in on Unity web page (different methods possible)
- Callback on service (with **code** and **state**)
- Client sends **code** to **Token Endpoint**
  - Receive an Access Token and ID Token in response
- Client gets information from **Userpoint Endpoint** (with tokens)
  - Email, name, other attributes

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?