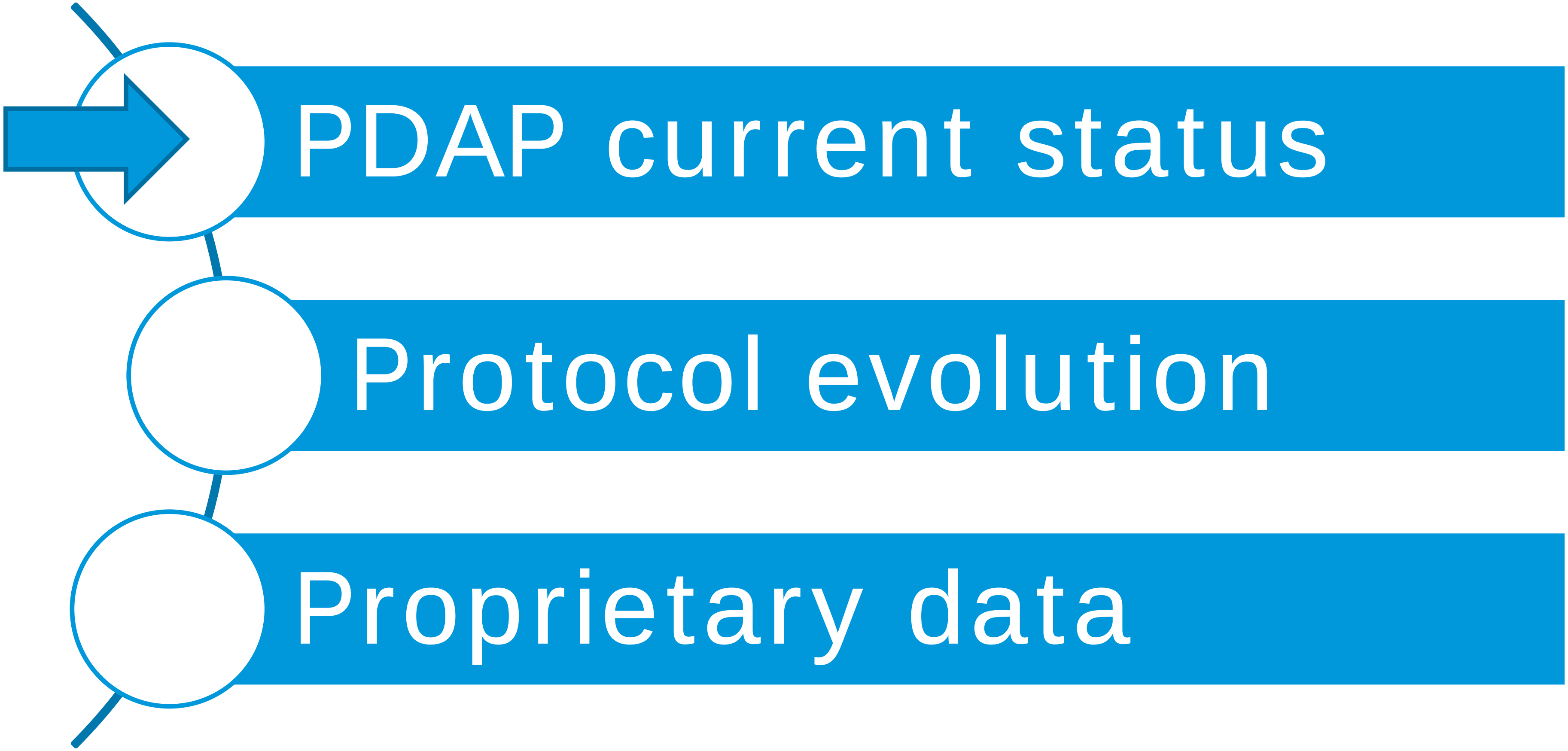
# PDAP Core Project: Status and Evolution

Jesús Salgado

ESA/PSA

17/07/2013



PDAP current status

Protocol evolution

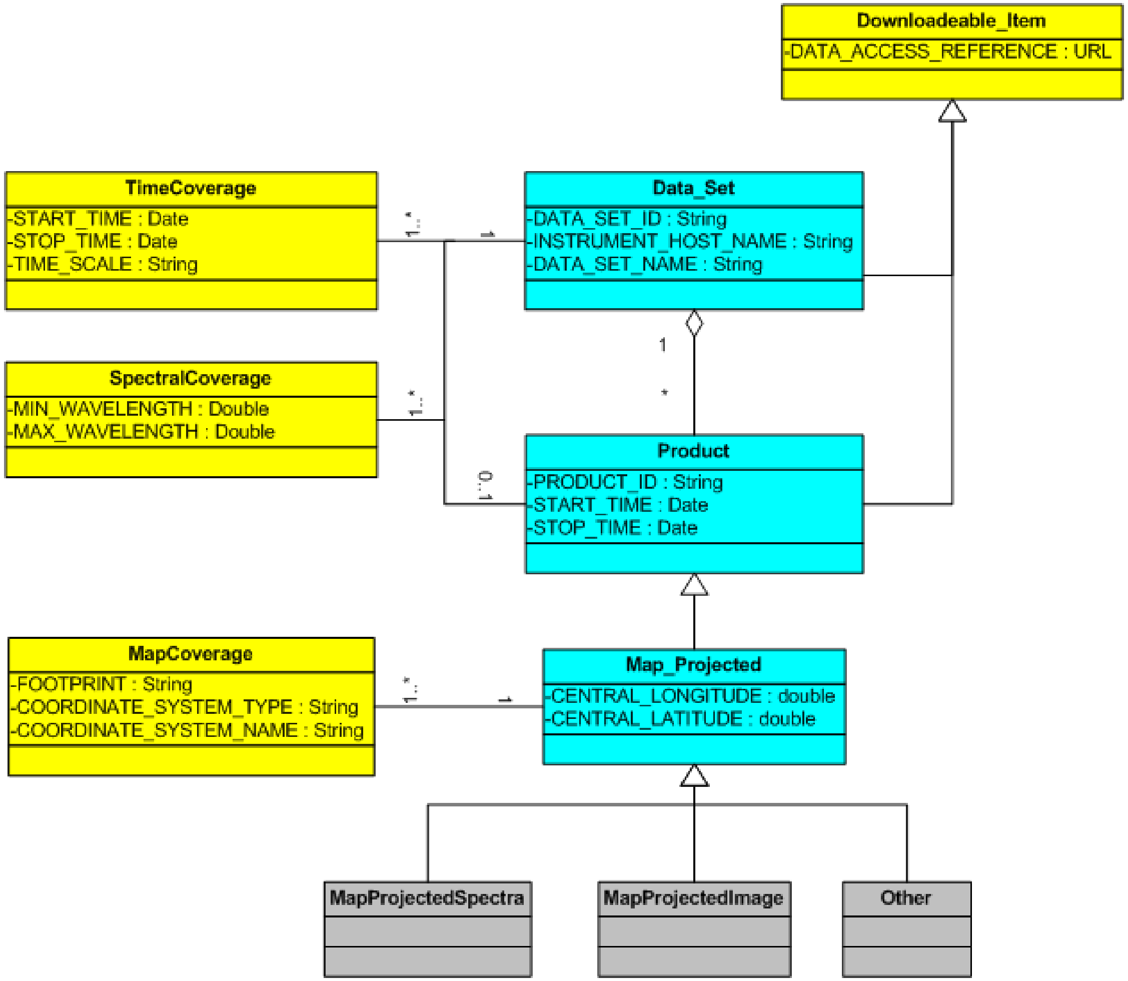
Proprietary data

# PDAP v1.0 status

- PDAP updated version 16/04/2013
- This version incorporates changes requested in the RFC PDAP process
- Main comments received from Baptiste Cecconi and Paul Ramirez
- Problems not solved:
  - Proprietary data
  - Arrays, multiplicity, hierarchy
- No comments received to this later version
- Next step: Provide agreement (or disagreement) at SC level from the different organizations in order to promote PDAP as Recommendation

IPDA PDAP RFC page

# PDAP Core UML



Downloadeable_Item
-DATA_ACCESS_REFERENCE : URL

TimeCoverage
-START_TIME : Date
-STOP_TIME : Date
-TIME_SCALE : String

Data_Set
-DATA_SET_ID : String
-INSTRUMENT_HOST_NAME : String
-DATA_SET_NAME : String

SpectralCoverage
-MIN_WAVELENGTH : Double
-MAX_WAVELENGTH : Double

Product
-PRODUCT_ID : String
-START_TIME : Date
-STOP_TIME : Date

MapCoverage
-FOOTPRINT : String
-COORDINATE_SYSTEM_TYPE : String
-COORDINATE_SYSTEM_NAME : String

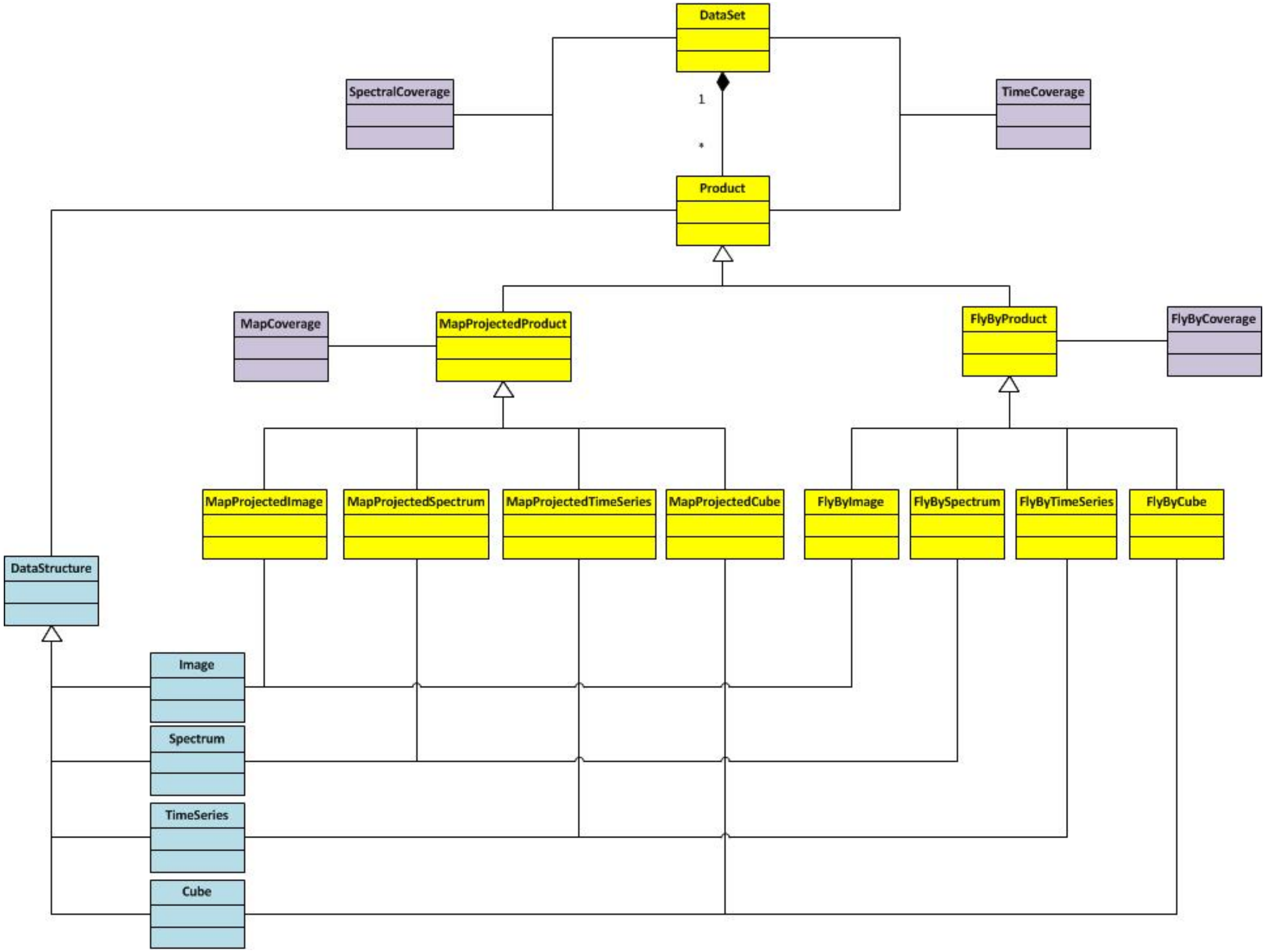
Map_Projected
-CENTRAL_LONGITUDE : double
-CENTRAL_LATITUDE : double

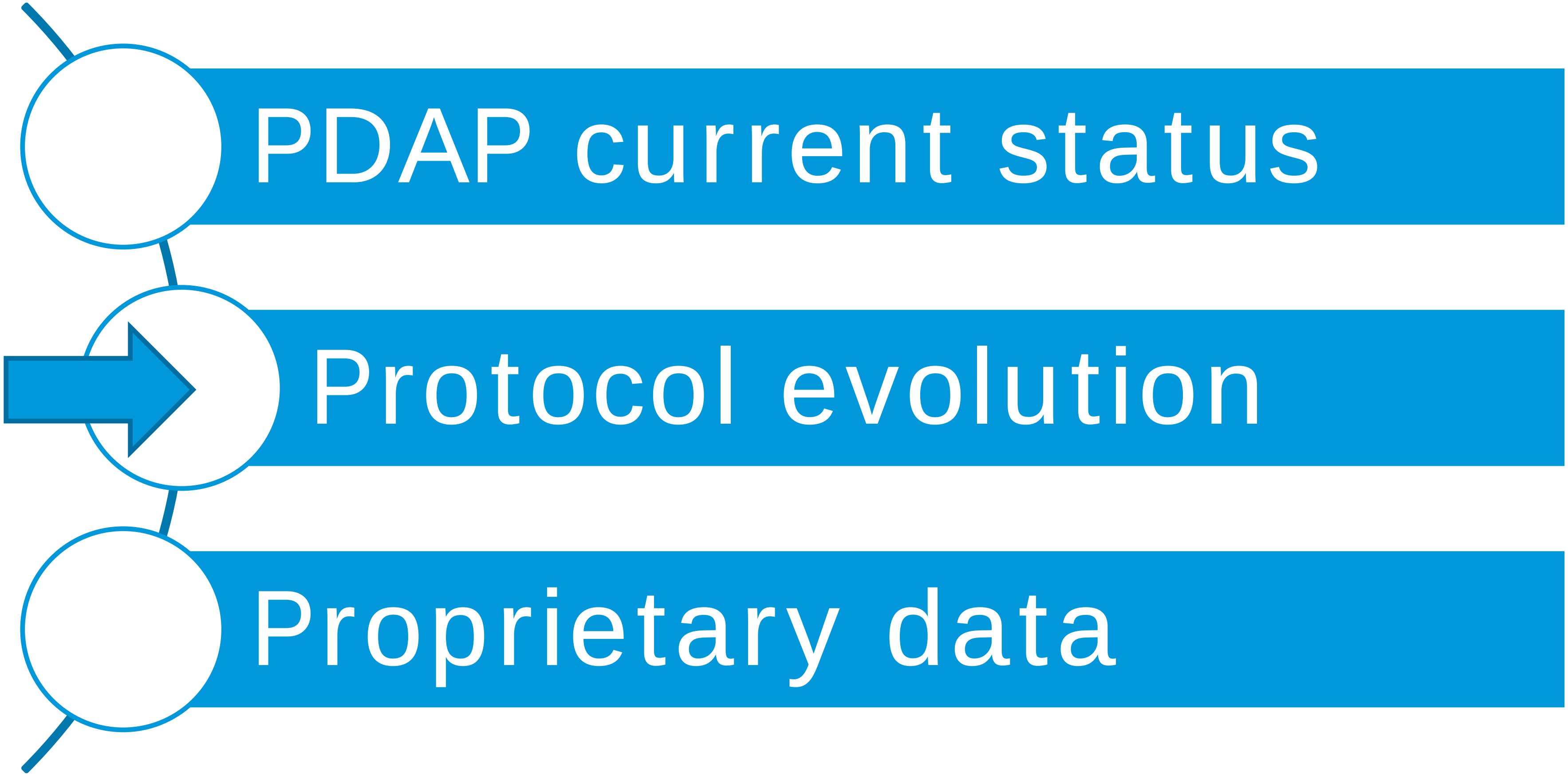
MapProjectedSpectra

MapProjectedImage

Other

# PDAP extended UML proposal





PDAP current status

Protocol evolution

Proprietary data

# PDAP / PDS4 interrelation

- ❑ See Steve’s presentation
- ❑ Any protocol in planetary context should have a correct mapping to PDS data as most of the data is in this format, either PDS3 and, in the future, PDS4
- ❑ Other possible DMs (like, e.g. IDIS) should be also supported by mapping
- ❑ This specific UML agnostic protocol approach produce that not always the keywords will have a 1-1 relationship or the “exact” keyword name

# IVOA Protocols

- ❑ IVOA provides a set of specifications that could be reuse for planetary data
- ❑ Some of the IPDA members have another “hat” at IVOA, so the interrelation could be quite flexible
- ❑ Some of the specifications could be also “endorse” by IPDA with certain restrictions

- ❑ Two different families of access protocols:
  - S*AP (Simple * Access Protocols)
  - TAP

# IVOA Protocols (II)

- S*AP protocols are, usually, two steps protocols
  - Metadata Query
  - Retrieval URLs
- Easy to implement
- In some way, these protocols are object oriented
- Make use of a simple query language (PQL- Parameter Query Language) although they can be extended
- Some examples: SIAP, SSAP and SLAP
- PDAP is, in some way, a S*A protocol

# IVOA Protocols (III)

- ❑ TAP (Tabular Access Protocol) is a simple protocol that allows queries using a relational approach
- ❑ Several query languages can be used but ADQL (Astronomical Data Query Language. Server ***should*** have a RDBMS

  *REQUEST=doQuery*

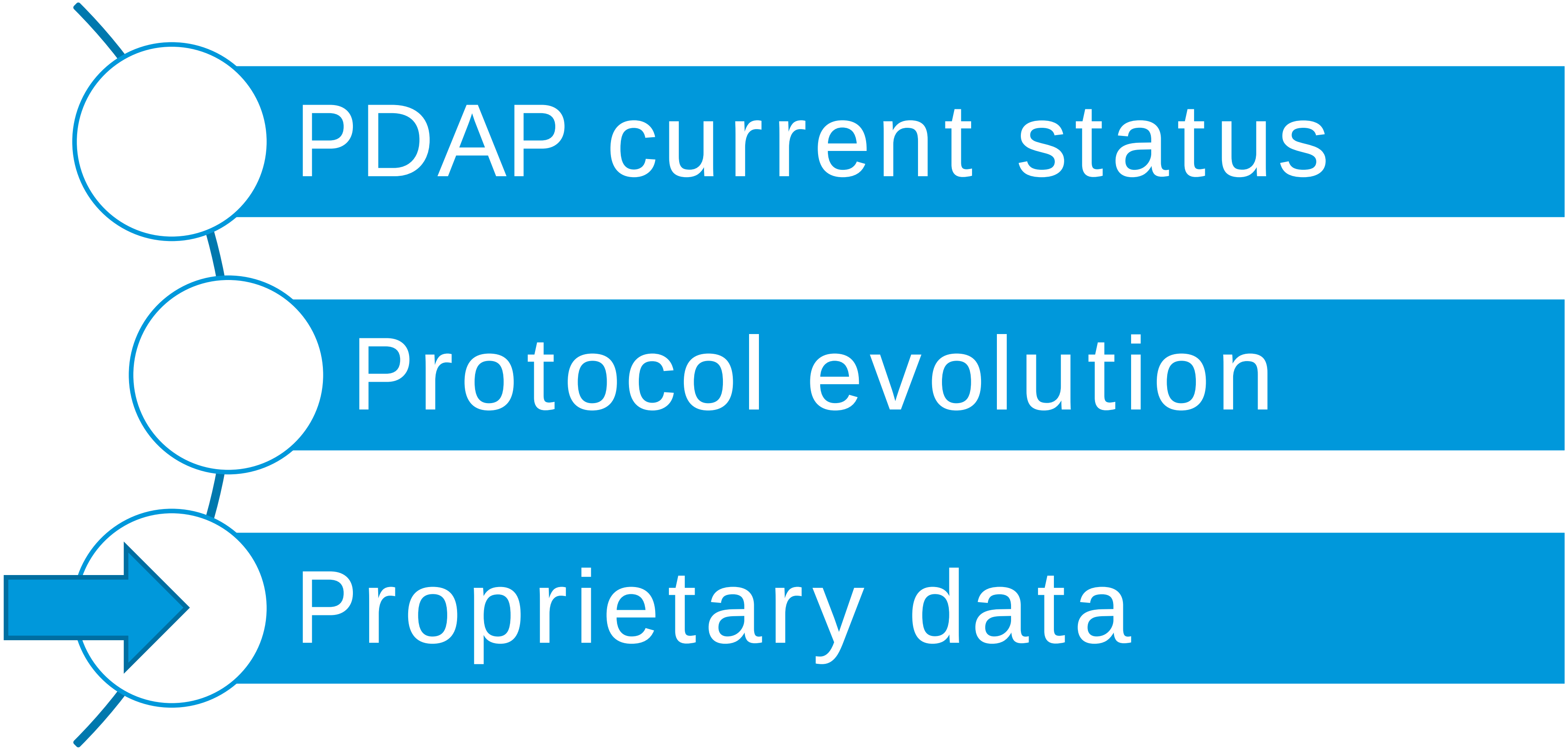
  *LANG=ADQL*

  *QUERY=select * from ivoa.ObsCore where*

  *INTERSECTS(s_region, CIRCLE('ICRS', 180, 5, 2)) = 1*

- ❑ Relational approach and data model is not closely related to the protocol
- ❑ Output in VOTable, single table
- ❑ VO-DML (a new standard from IVOA DM group) will try to solve this issue

VO-DML example



PDAP current status

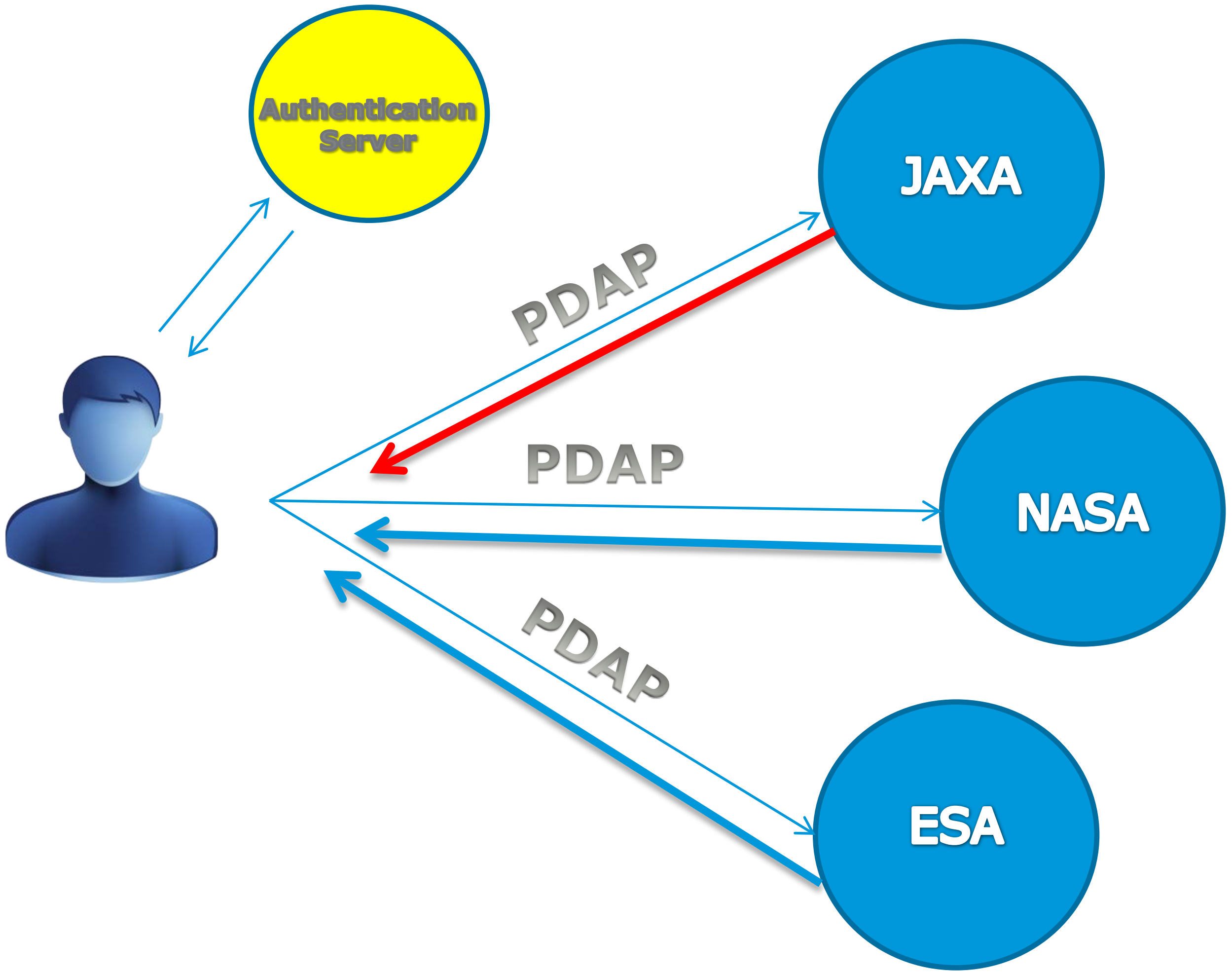
Protocol evolution

Proprietary data

# Credentials in IPDA

- ❑ Main issue raised on PDAP RFC was related to the access to proprietary data in the planetary environment
- ❑ (JAXA + ESA/Bepi Colombo)
- ❑ This has not been included in first PDAP version due to the complexity
- ❑ This issue does not affect only PDAP but any other possible access protocol (or PDAP evolution) in the planetary context
- ❑ From IVOA we have:
  - ❑ Single Sign-on recommendation
  - ❑ Credentials delegation protocol
- ❑ However, in this particular case, the protocols provided by IVOA are not too detailed as the main access to VO data is to public data

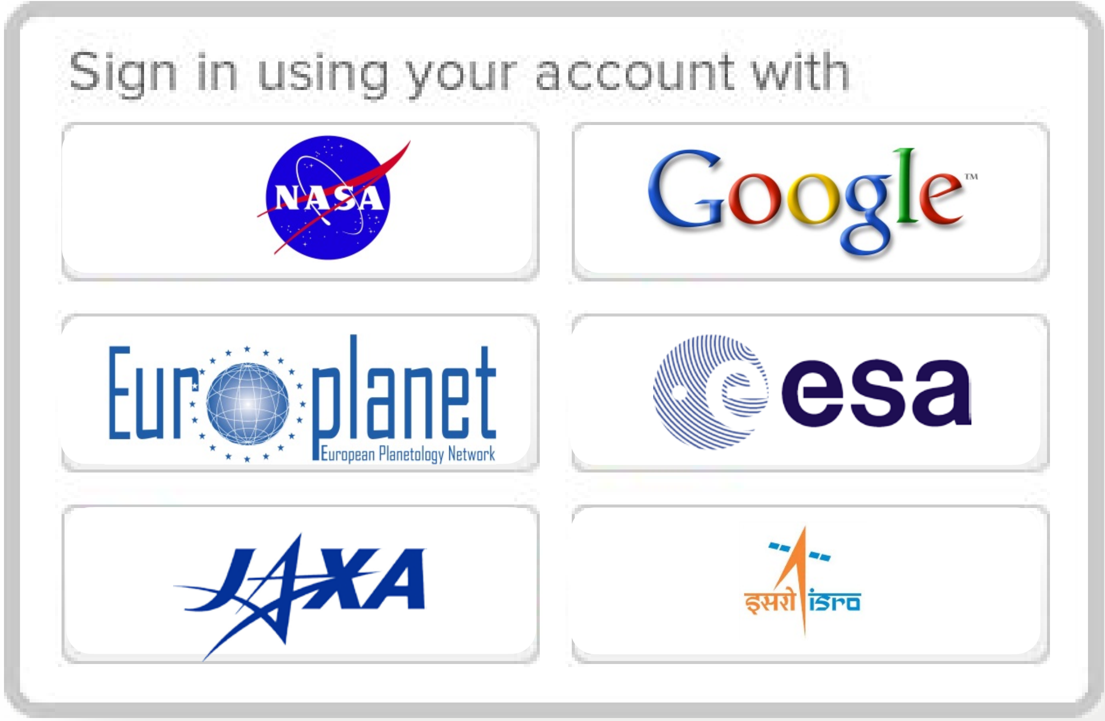
# The problem



# CAS (Central Authentication Service)

- ❑ CAS: is a single sign-on protocol for the web. It allows a user to access multiple applications providing their credentials only once
- ❑ It involves three parties: client web browser, web applications requesting authentication and the CAS server
- ❑ CAS server usually checks the credentials using a secure username/password check (e.g. Kerberos)
- ❑ It makes use of security tickets
- ❑ Merge Accounts (?)
- ❑ Drawback: Usually, widgets are more focused on web applications. It looks that this could be useful but IPDA should endorse a more low level protocol

# Log in with your preferred credentials



Sign in using your account with

# OpenID

- ❑ OpenID: is an open standard that allows users to be authenticated on a certain co-operating system using a third party service
- ❑ **It does not rely on a central authority to authenticate user’s identity**
- ❑ It allows a range of approaches on how to authenticate users from passwords to new ones (e.g. smart cards)
- ❑ Possible approach for IPDA (one OpenID per organization)
- ❑ Final check is done through a “shared secret” or a “check authorization” call
- ❑ Drawback: You can trust big organizations OP (e.g. google) but Google could not trust you (this could be not too important for IPDA)

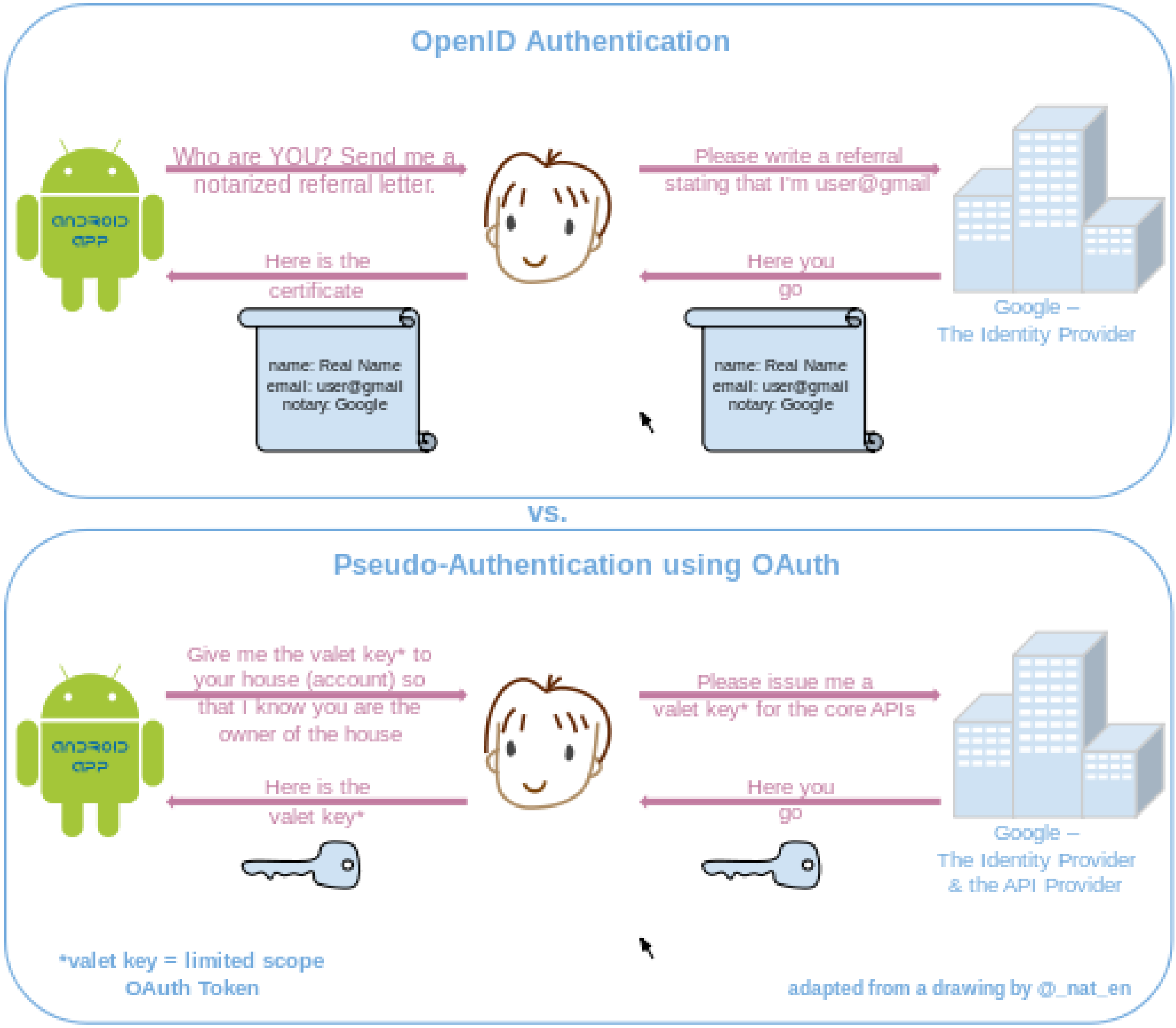
# OpenID Drawbacks

- You can trust big organizations OP (e.g. google) but Google could not trust you (this could be not too important for IPDA)
- Although it is a quite stable protocol (no relevant updates from 2007) and there are several libraries to remove complexity, version 2.0 looks difficult to understand and implement.
- It requires more than one handshake in order to obtain data stored in one server (main purpose of SSO in IPDA). In fact, it requires collaboration from OAuth (next slides)
- Future new standard called OpenID Connect is ongoing

# OAuth

- ❑ OAuth: is an open standard for authorization. OAuth provides a method for clients to access server resources on behalf of a resource owner. It also provides a process for end-users to authorize third-party access to their server resources without sharing their credentials
- ❑ **Authorization methods looks to be a must on IPDA**
- ❑ It can be considered complementary to OpenID
- ❑ Drawback: Could it be not enough? It is usually promoted to login in social networks as the primary authentication method and then use OAuth to access resources. We already have our own authorization credentials...

# Solutions: OpenID versus OAuth



OpenID Authentication

Who are YOU? Send me a notarized referral letter.

Please write a referral stating that I'm user@gmail

Here is the certificate

Here you go

name: Real Name
email: user@gmail
notary: Google

name: Real Name
email: user@gmail
notary: Google

Google –
The Identity Provider

vs.

Pseudo-Authentication using OAuth

Give me the valet key* to your house (account) so that I know you are the owner of the house

Please issue me a valet key* for the core APIs

Here is the valet key*

Here you go

Google –
The Identity Provider
& the API Provider

*valet key = limited scope
OAuth Token

adapted from a drawing by @_nat_en

# Use of OAuth

## List of OAuth service providers:

- Amazon 2.0[19]
- Facebook 2.0 draft 12[4]
- Google 2.0
- Google App Engine 1.0a [21]
- Instagram 2.0
- LinkedIn 1.0a, 2.0[22]
- Microsoft (Hotmail, Windows Live, Messenger, Xbox) 2.0
- MySpace 1.0a
- PayPal 2.0
- Twitter 1.0a, 2.0[27]
- Ubuntu One 1.0
- XING 1.0[29]
- Yahoo! 1.0a

# Proposal for a new project

- Create a project, including participants of the different IPDA members, with the following schedule:
  - Definition of the real needs and requirements for SSO and authorization/authentication within IPDA
  - Analyse the different alternatives and standard protocols that already exist
  - Propose a technical solution (that could include the endorsement of a SSO mechanism) for the IPDA
  - Implement a prototype to test the solution,  e.g. by creating a version of PDAP or TAP that access “proprietary” (real or not) data

## THANK YOU

Jesus Salgado

IPDA PDAP Project: Status and Evolution

Jesus.Salgado@sciops.esa.int