Affiliation registries

(talk listed in agenda as "centralize, centralize, centralize")

Guy Rixon

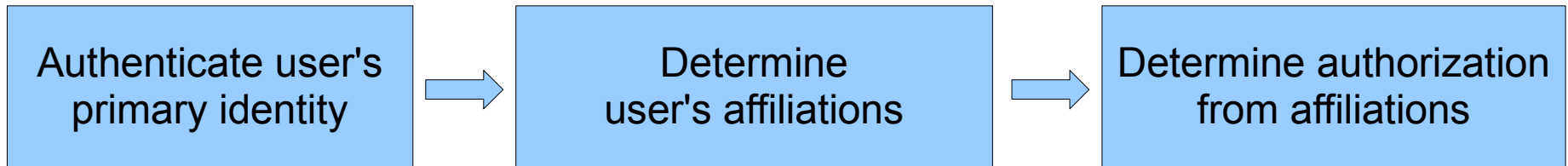Presentation to GWS-WG of IVOA, Baltimore, October 2008

Authorization *is* local

MG asked me to present the argument for **centralizing authorization decisions.**
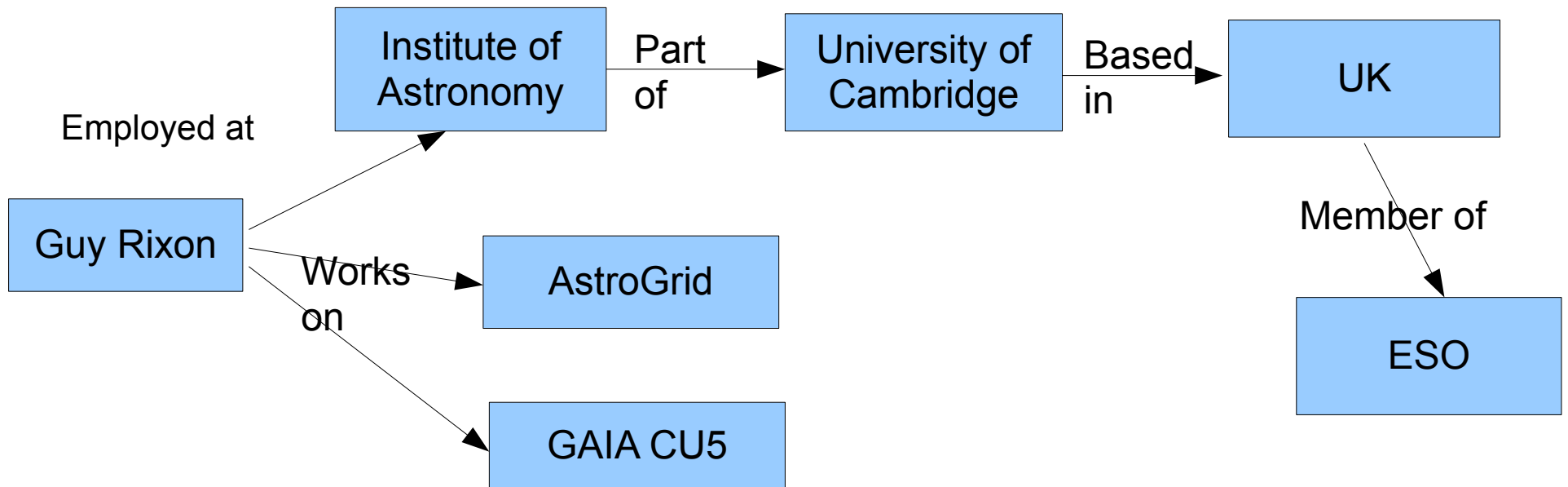
I know no such argument. Sorry.

However...

Affiliation is not authorization

Authenticate user's primary identity	→	Determine user's affiliations	→	Determine authorization from affiliations

A(A)AA:
Authentication, (affiliation), authorization, accounting

Affiliation can be a graph...

Kudos to Norman Gray for pointing this out

...or a list

- C=UK,O=AstroGrid,OU=IoA,CN=Guy Rixon is a member of user-groups:
  - IoA Cambridge
  - University of Cambridge
  - UK Astronomy
  - Affiliates of ESO-member states
  - AstroGrid
  - GAIA CU5

You can do affiliation locally

- Choose the graph or list form as suits you best

- Merge it with your authorization code if you like

- BUT: first consider these points:

  - Does it scale?

  - Is it nice for your users?

Scaling local management

Personal collaboration
~1 user

Research group
~10 users

University department
~100 users

Regional VObs project
~1000 users

International research
project ~1000 users

High-school students
~millions? ~billions?

Now assume, say, 10% turn-over per year to estimate the management work...

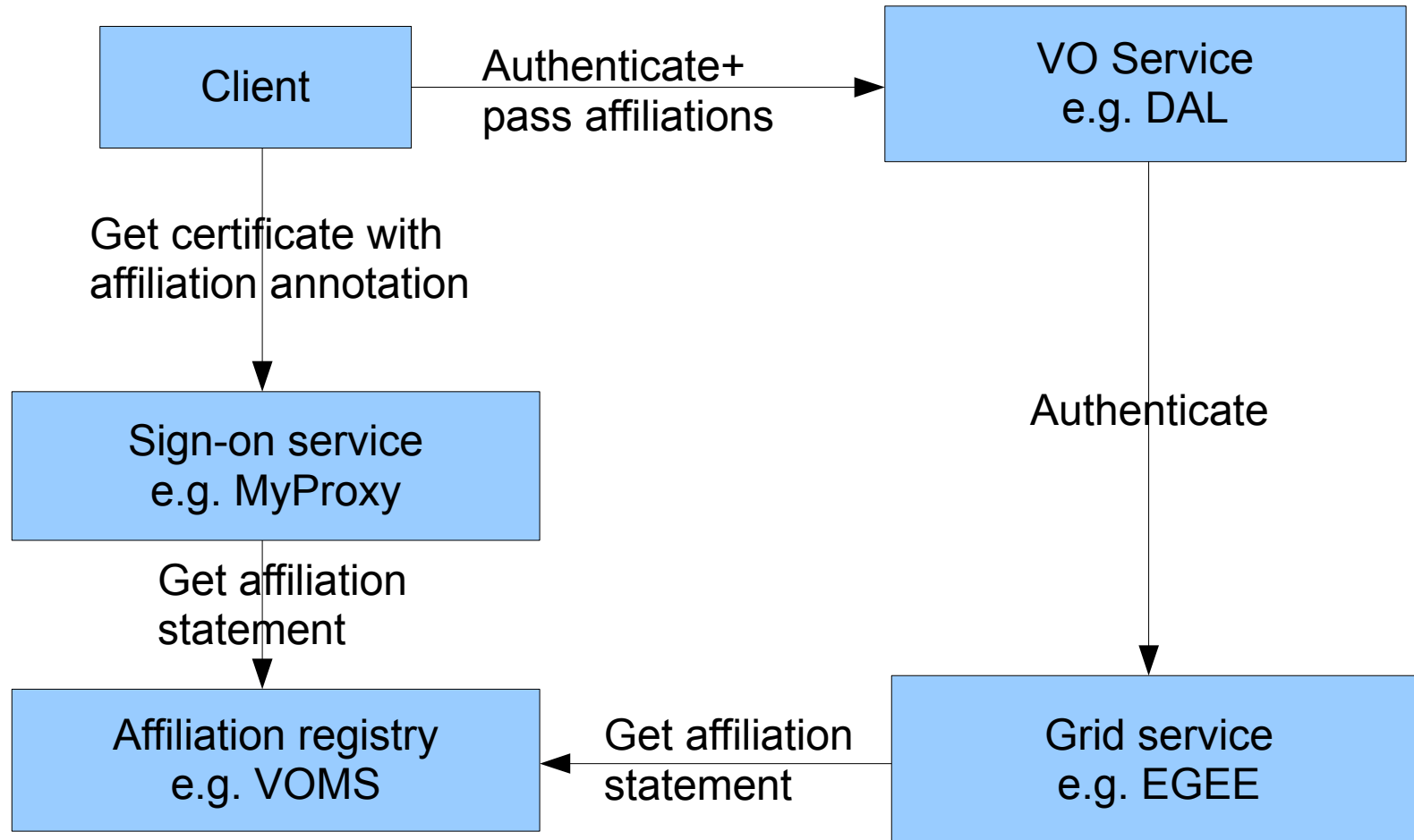# User experience with local management of affiliation

1) Get certified

2) Register certified identity with VObs ID provider (optional)

3) Try to use restricted resource; get refusal

4) Talk with colleagues; ask helpdesk; email VObs people; maybe pray

5) (Much later) Realize affiliations not known to service provider

6) Contact service provider; negotiate registration of affiliations

7) (Later) Finally use restricted resource

8) Repeat steps 3..7 for rest of VObs...

User experience with central management of affiliations

1) Get certified

2) Register certified identity with VObs ID provider (who also does your affiliations)

3) Use restricted resource

Local management; how?

Summary

- Authorization is always managed locally

- Affiliation can be managed locally or centrally

- Local management may or may not scale

- User experience with local management is poor

- User experience can be better with central management

- Central management implies some community service

  - Probably doesn't need an IVOA protocol