National e-Science Centre

Requirements for Repository Environments: Supporting User and Provider Friendly Single Sign-On Models

Prof. Richard O. Sinnott
National e-Science Centre
University of Glasgow, Scotland
r.sinnott@nesc.gla.ac.uk

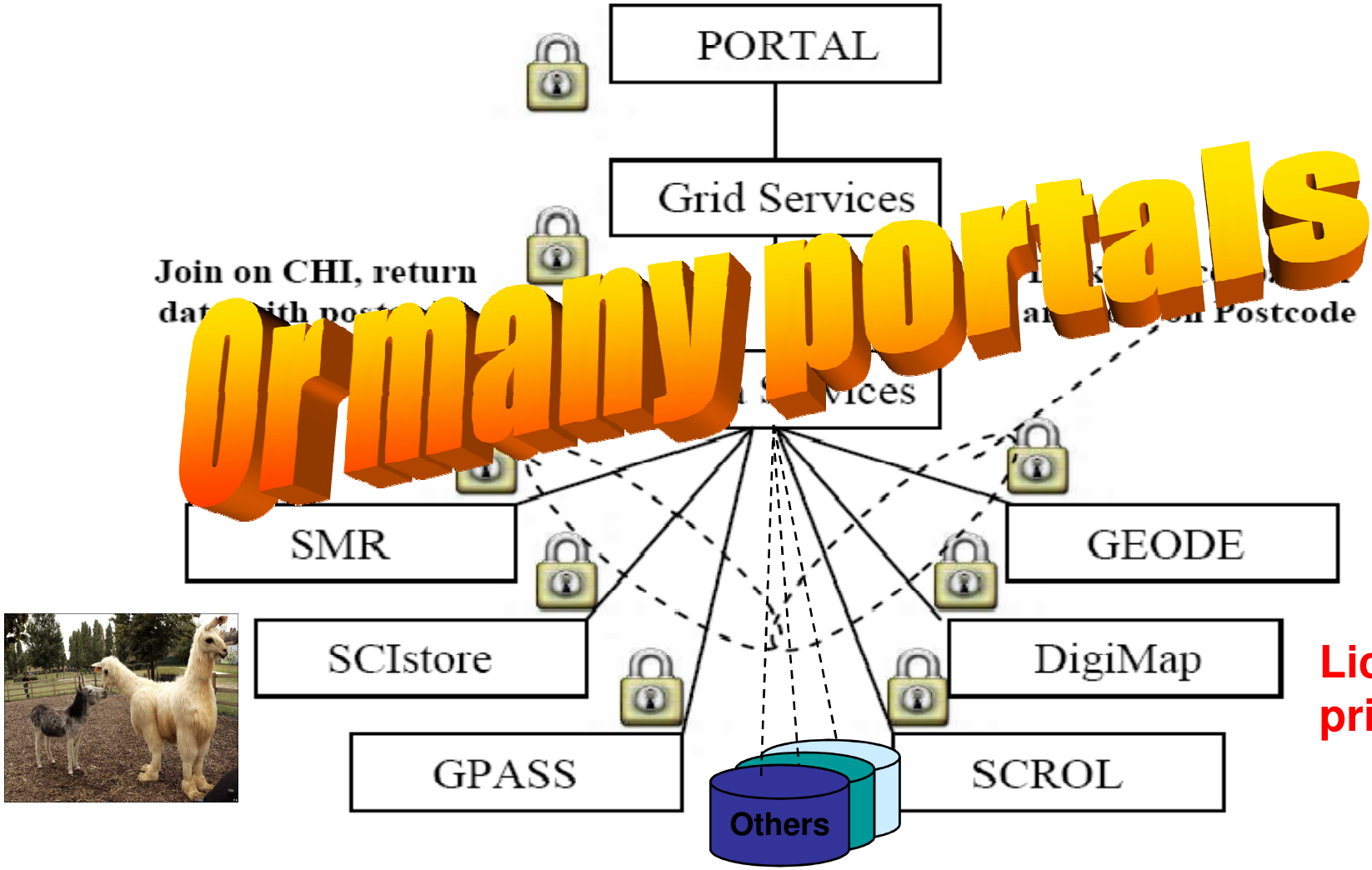
E-Infrastructures

National e-Science Centre

- Desirable features of e-Infrastructures:
  - Simplicity for end users
    - They want to do research not necessarily e-Research
  - Single sign-on for end users
    - Log-in once
  - Site autonomy and tool support for providers
    - Local policy definition and enforcement
  - Support research and researchers
    - Often at risk of being non-sexy
- Observation
  - Data Grids much harder to create and maintain than compute Grids
    - Most of my customers want data Grids!!!

Security-oriented Socio-, Geo-, Clinical Data Infrastructures

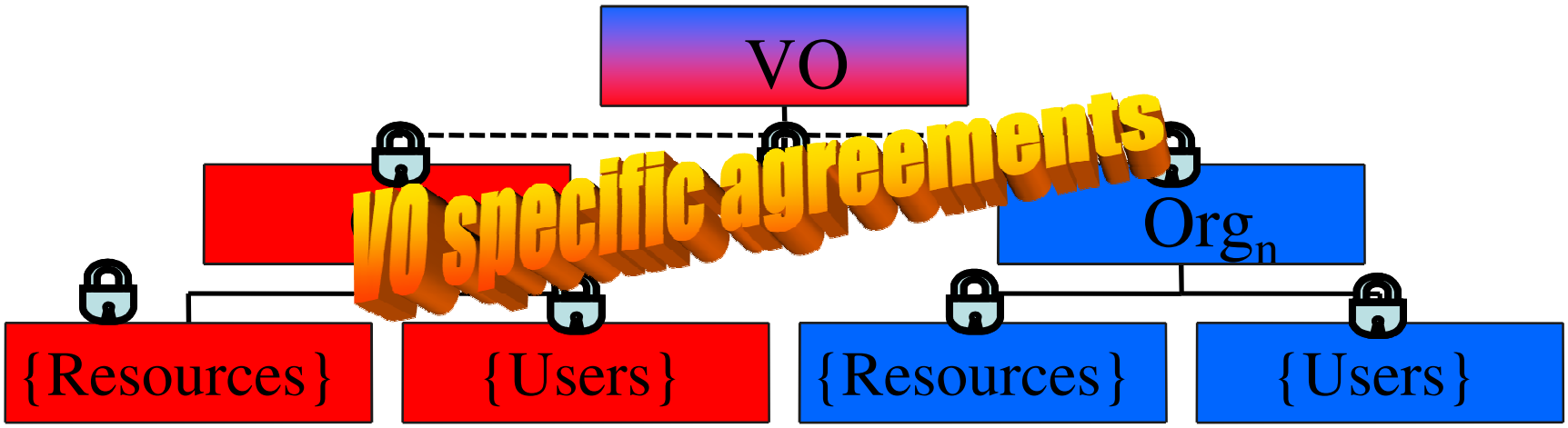
National e-Science Centre



Virtual Organisations

National e-Science Centre

- Key to this is to *dynamically* establish and managing VOs
  - collection of distributed resources shared by collection of users from one or more organizations
    - Provides conceptual framework for rules and regulations for resources that are to be offered/shared between VO institutions/members
      - » Clinical domain **much** greater emphasis on expression and enforcement of rules and regulations (policies)
      - » Less emphasis on dynamic (you don't/shouldn't find resources on the fly, you care very much which users are in the VO and what their role is…)

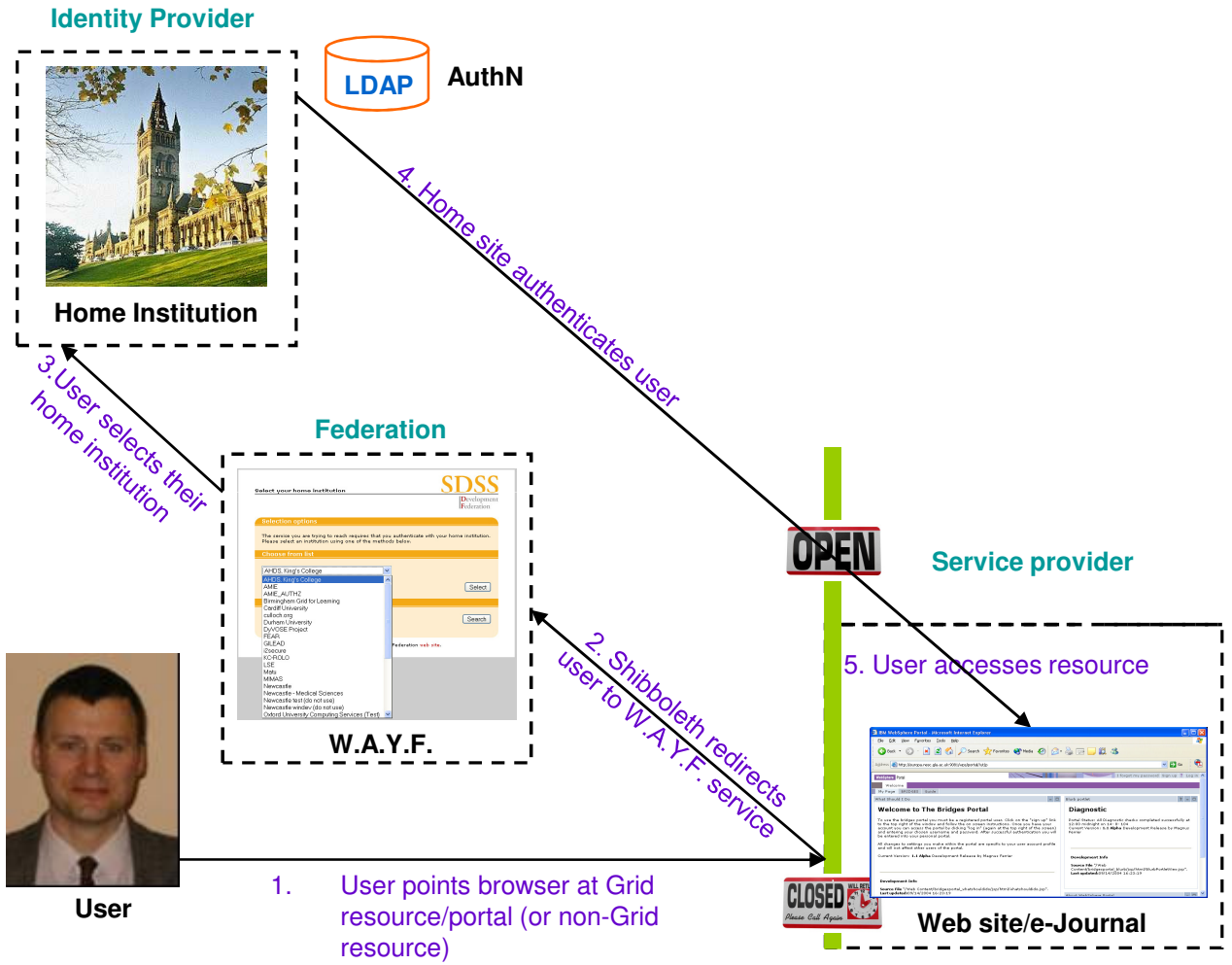


AAAA

National e-Science Centre

- Grid Security
  - AAAA
- Users like usernames/passwords
  - Provide them (once!)
- Users don't like/understand X.509 based PKI
  - Forget training, education for most users!
    - *$> openssl pkcs12 -in cert.p12 -clcerts -nokeys -out usercert.pem!*
  - The vast majority most certainly won't jump through hoops to get on the Grid
    - "me-Science" culture
  - Should all be transparent to end users and aligned with the way that they want to work/access resources
    - Access Management Federation (Shibboleth) + authZ technologies

Improved authentication for non-VO-based Shibboleth



Log-in once and roam

Shibboleth and Dynamic VOs?

National e-Science Centre

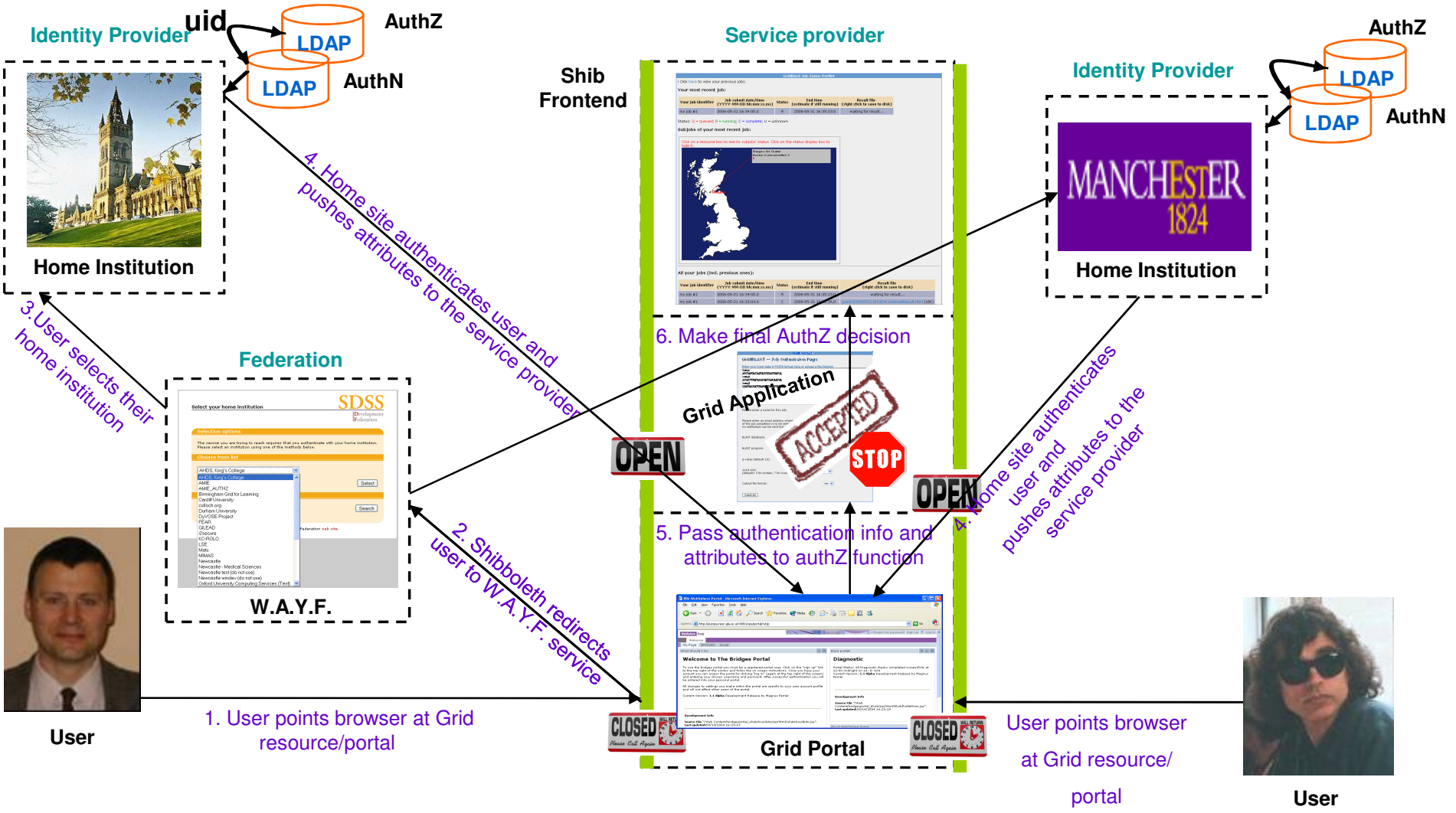
- UK Shibboleth federation based around small set of pre-agreed attributes based on eduPerson schema
  - *eduPersonScopedAffiliation*: indicates the user's relationship (e.g., staff, student, etc) within the institution;
  - *eduPersonTargetedID*: needed when an SP is presented with an anonymous assertion only, e.g. eduPersonScopedAffiliation. This attribute provides a persistent user pseudonym;
  - *eduPersonPrincipalName*: used where a persistent user identifier consistent across different services is needed;
  - *eduPersonEntitlement*: enables an institution to assert that a user satisfies an additional set of specific conditions that apply for access to a particular resource
    - Note that not all sites support ALL of these attributes!!!
- Grid vision for dynamic virtual organisations
  - Add, remove, change people, institutes, their privileges on the fly for changing sets of resources as required by the VO

_ A _ _ using technologies like PERMIS

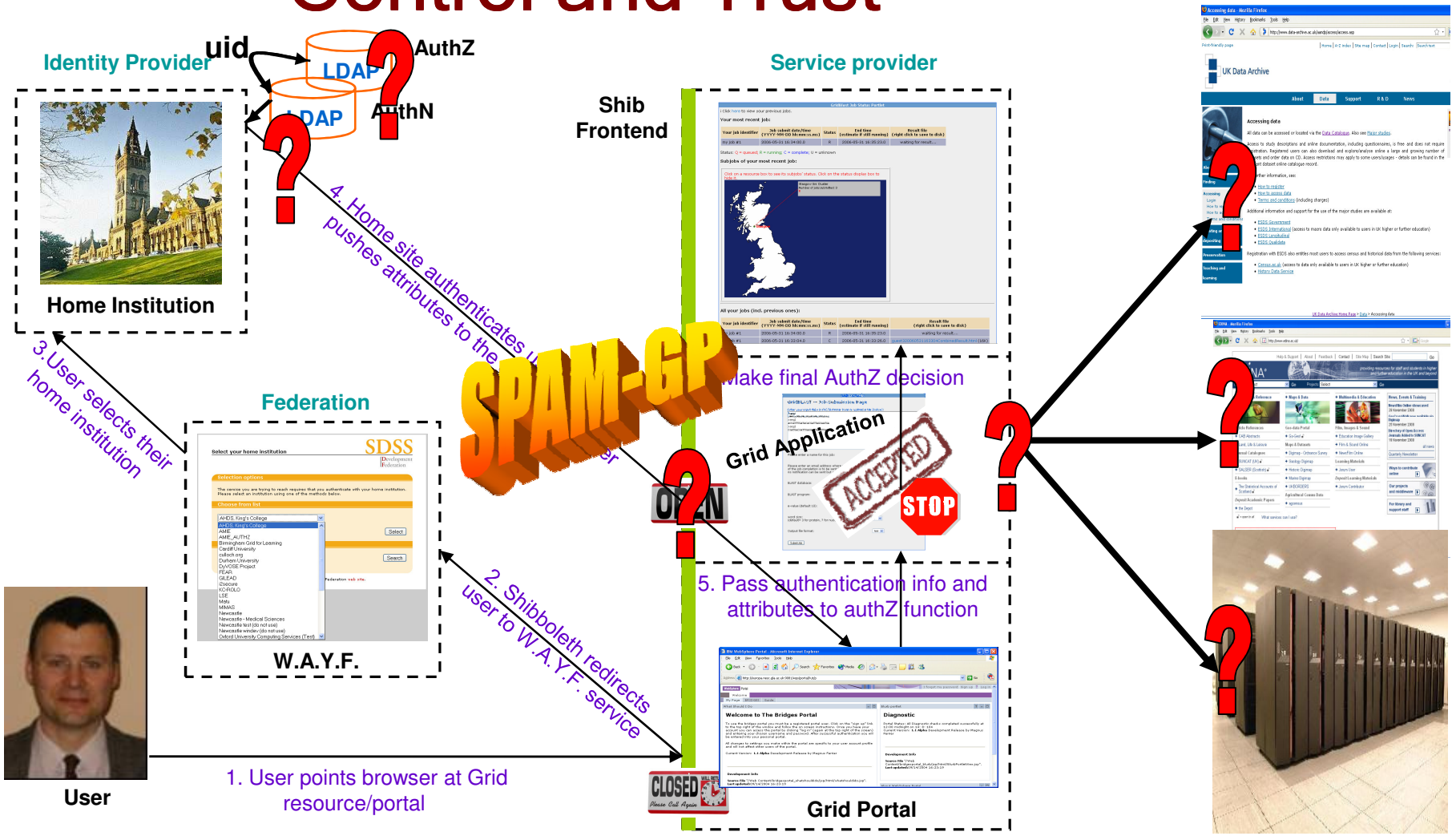
National e-Science Centre

- Role Based Access Control
  - Basic idea is to define:
    - *roles* applicable to specific VO
      - roles often hierarchical
        - » Role X ≥ Role Y ≥ Role Z
        - » Manager can do everything (and more) than an employee can do who can do everything (and more) than a trainee can do
    - *actions* allowed/not allowed for VO members
    - *resources* comprising VO infrastructure (computers, data etc)
  - A policy then consists of sets of these rules
    - *{ Role x Action x Target }*
      - » Can user with VO role X invoke service Y on resource Z?
    - Policy itself can be represented in many ways,
      - » e.g. XML document, SAML, XACML, …
    - Standards on when/where these used (PEP) and enforced (PDP)
  - Should all be transparent to end users!
  - *Shibboleth and advanced authZ solutions now make this possible*

Shibboleth Federated VO-based Approach



Privileges, Resources, Access Control and Trust



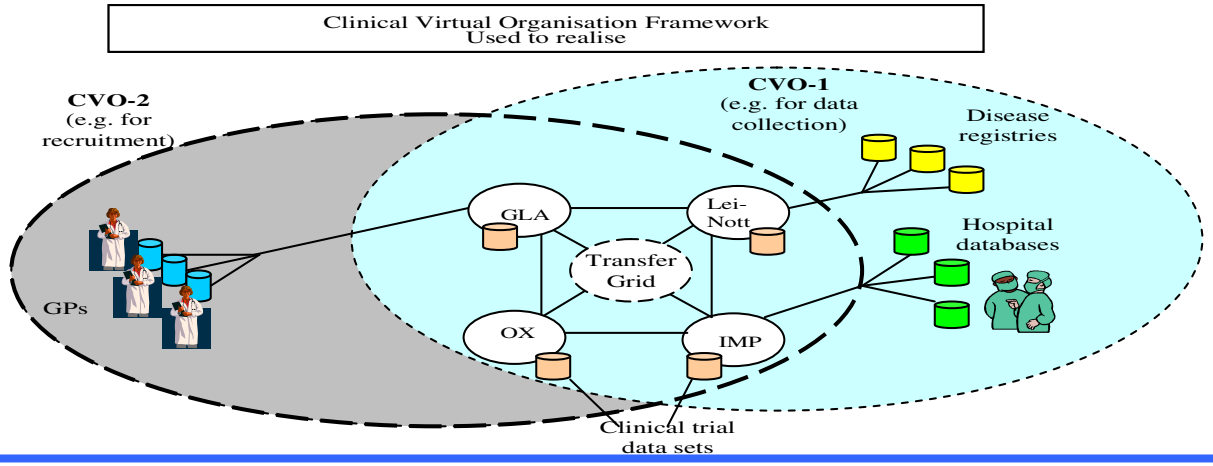
National e-Science Centre

Clinical, Social, Geo Background Projects

VOTES

National e-Science Centre

- Virtual Organisations for Trials and Epidemiological Studies
  - 3 year (£2.8M) MRC funded project started October 2005
  - Plans to develop *framework for producing Grid infrastructures* to address key components of clinical trial/observational study
    - Recruitment of potentially eligible participants
    - Data collection during the study
    - Study administration and coordination
      - Involves Glasgow, Oxford, Leicester/Nottingham, Manchester, Imperial
        - » Strong links with UK Biobank

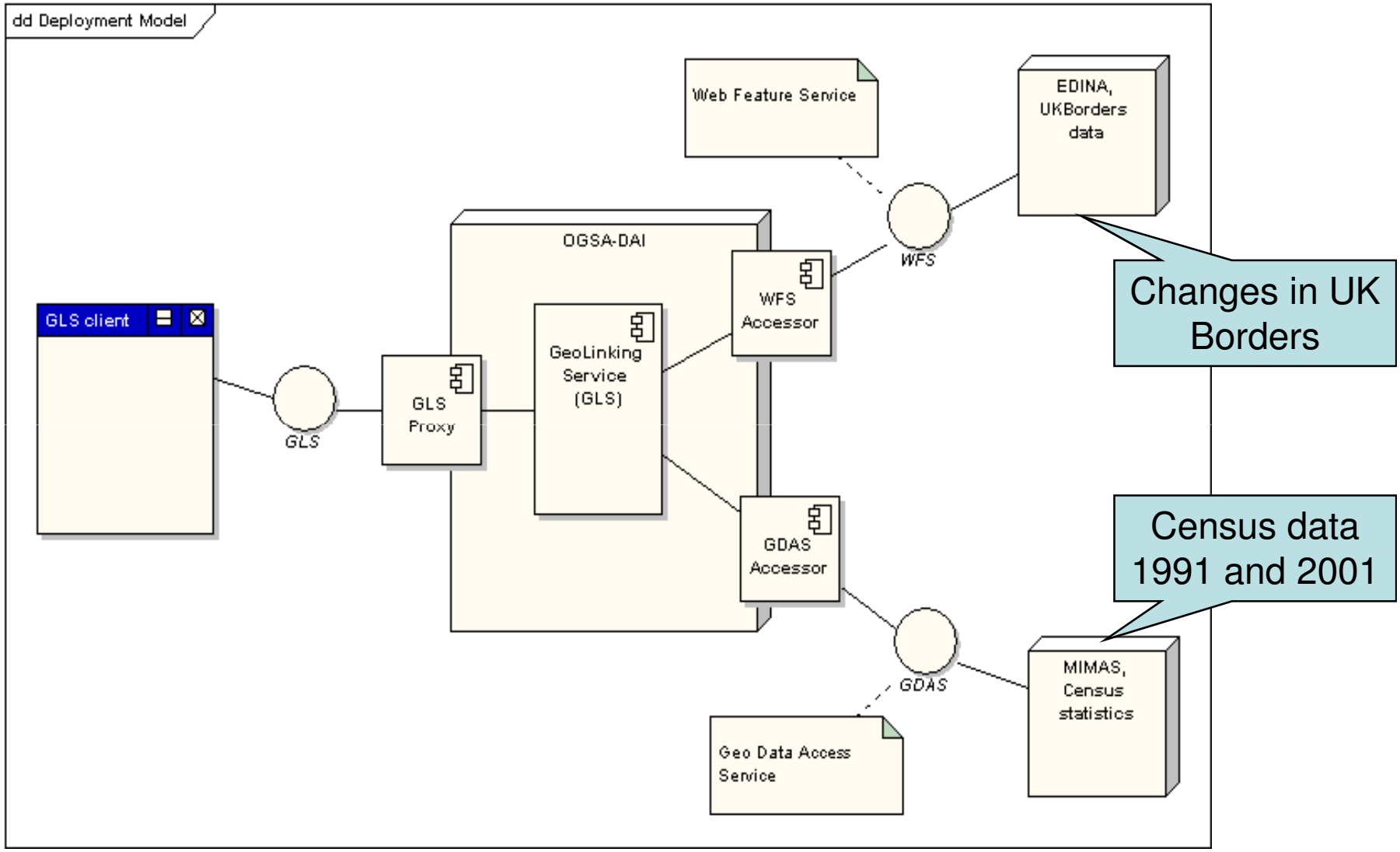


DAMES

- Data Management Through e-Social Science (DAMES)
- ESRC National Centre for e-Social Science node
  - Plans to provide services for accessing, analysing, recoding, linking, integrating… a variety of data sets
    - Social science data sets
      - Occupational data classifications
        - » Builds on GEODE project
      - Educational data sets
      - Ethnic data sets
      - E-Health data sets
        - » Especially related to mental health
    - Many of these data sets have strict access restrictions
      - (especially e-Health data sets)

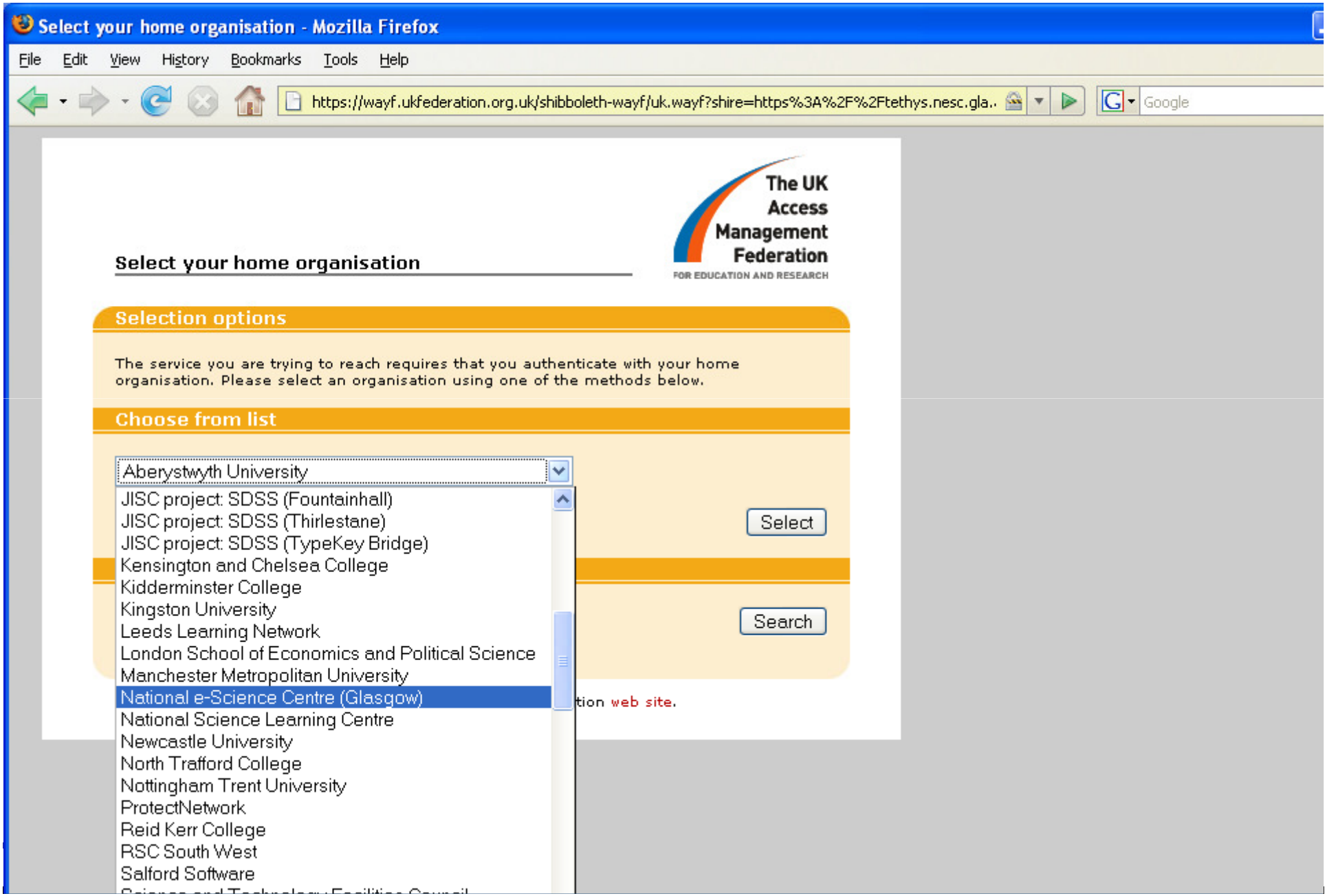
SeeGEO Project

National e-Science Centre

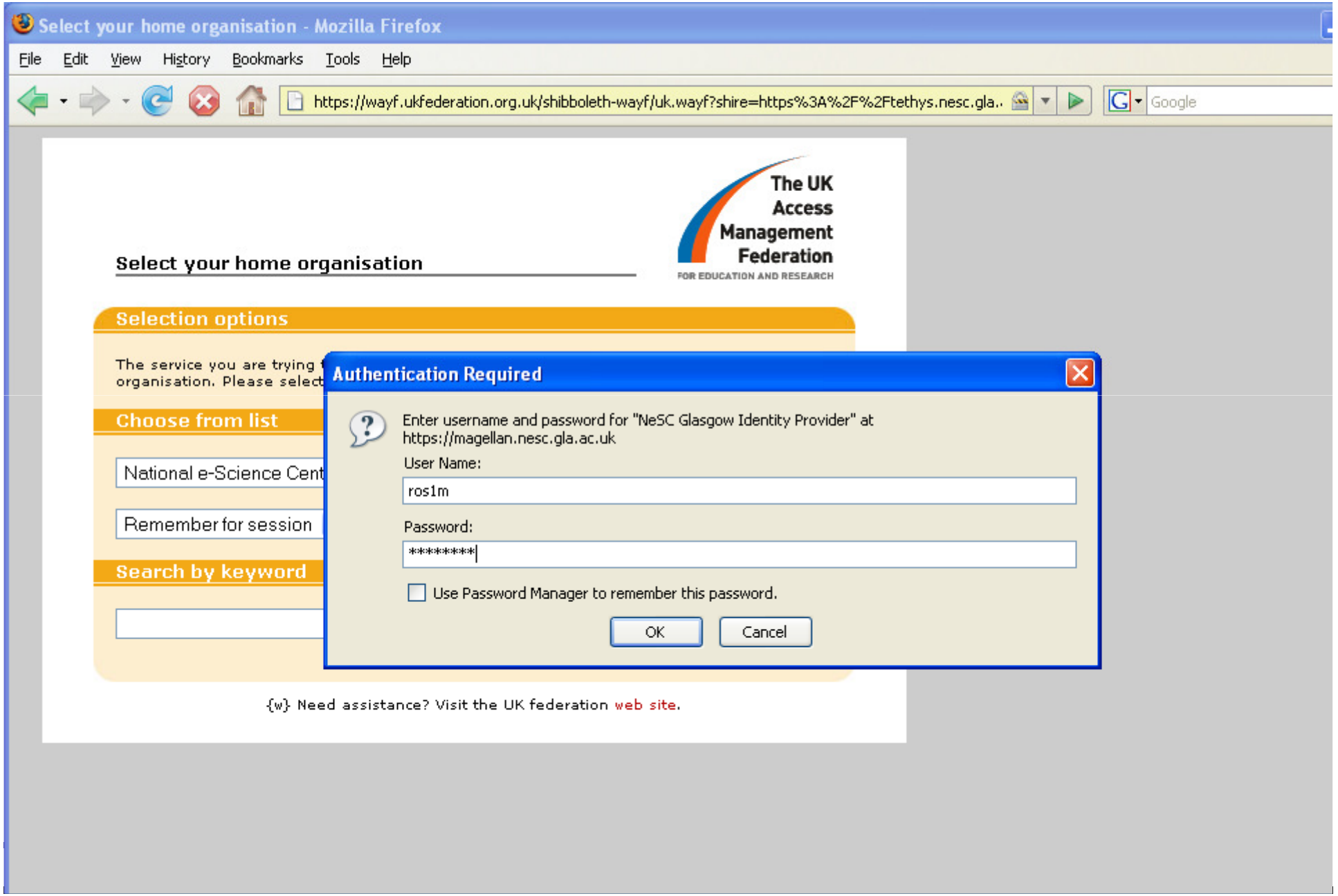


User attempts to access clinical trials portal

National e-Science Centre



National e-Science Centre



GridSphere Portal - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://tethys.nesc.gla.ac.uk/gridsphere/gridsphere

Google

gridsphere portal framework

English

VOTES portlet | ESPE portlet | ESPE Admin portlet | Shibboleth User Information | Portal Admin Entry

Data Federation

Distributed Data Framework

Clinical Trial Query Portlet

Select a trial that you would like specific information on.

Select a specific clinical trial

votes1

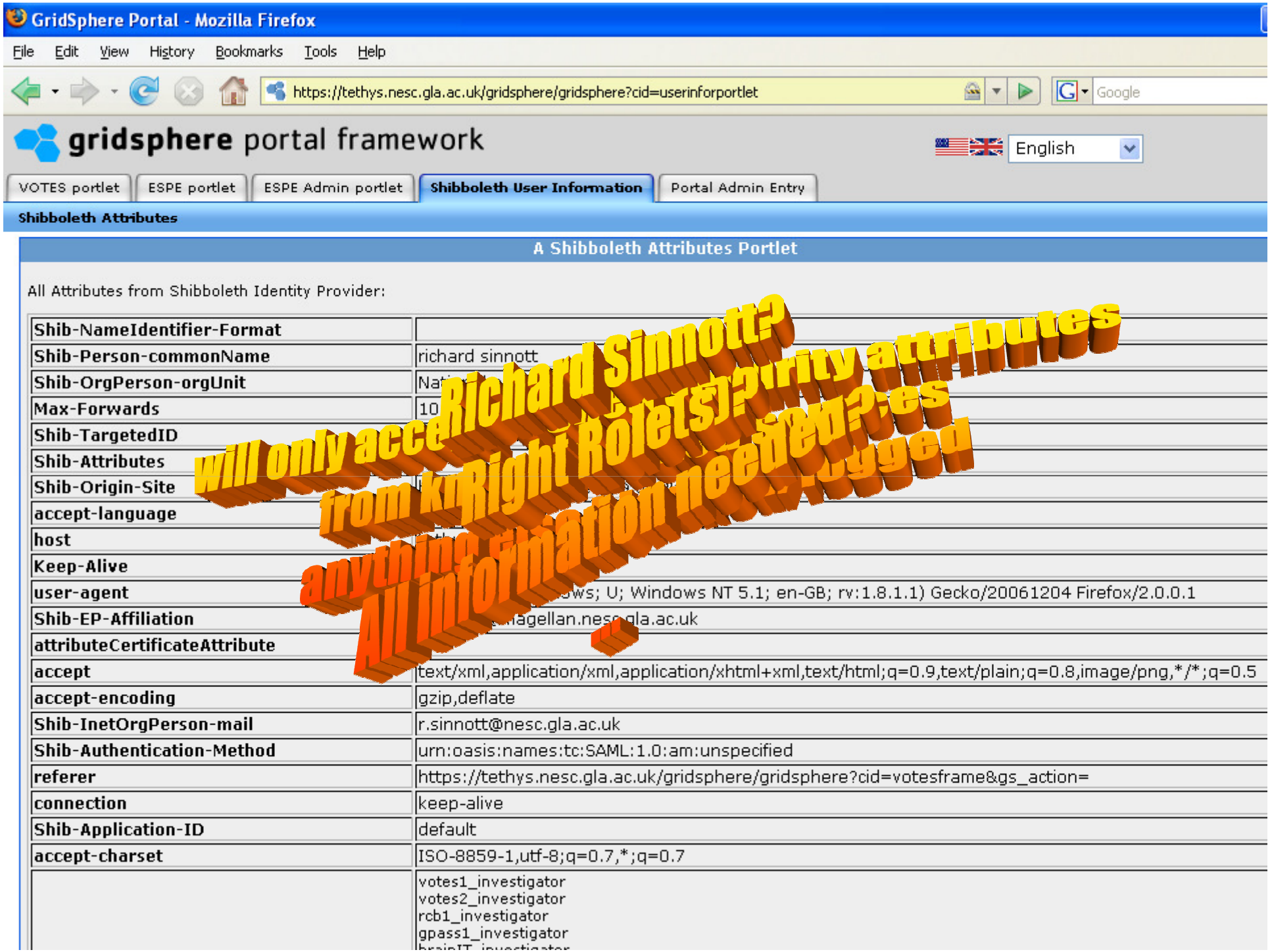
votes1
votes2
rcb1
brainIT
gpass1

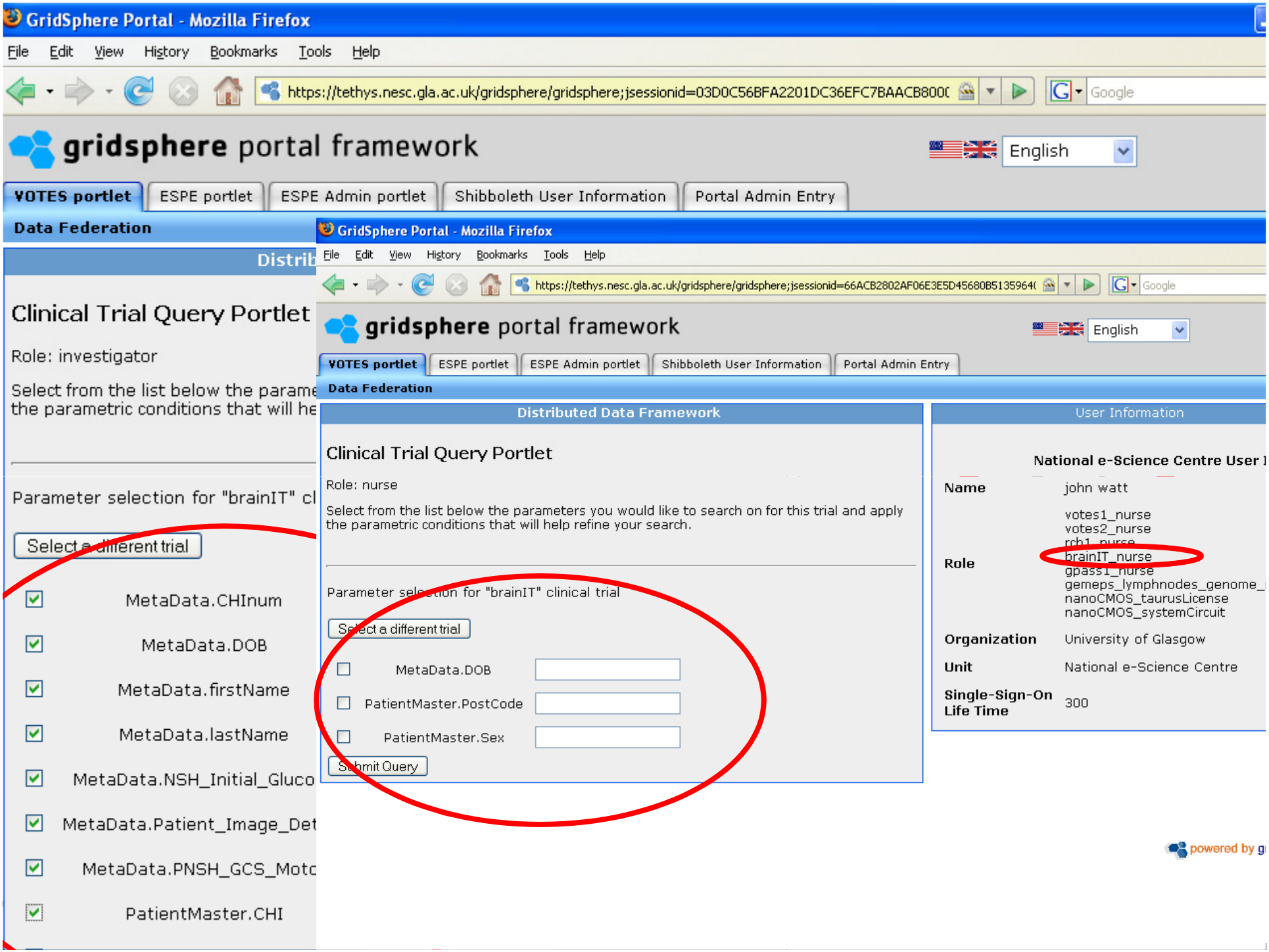
User Information

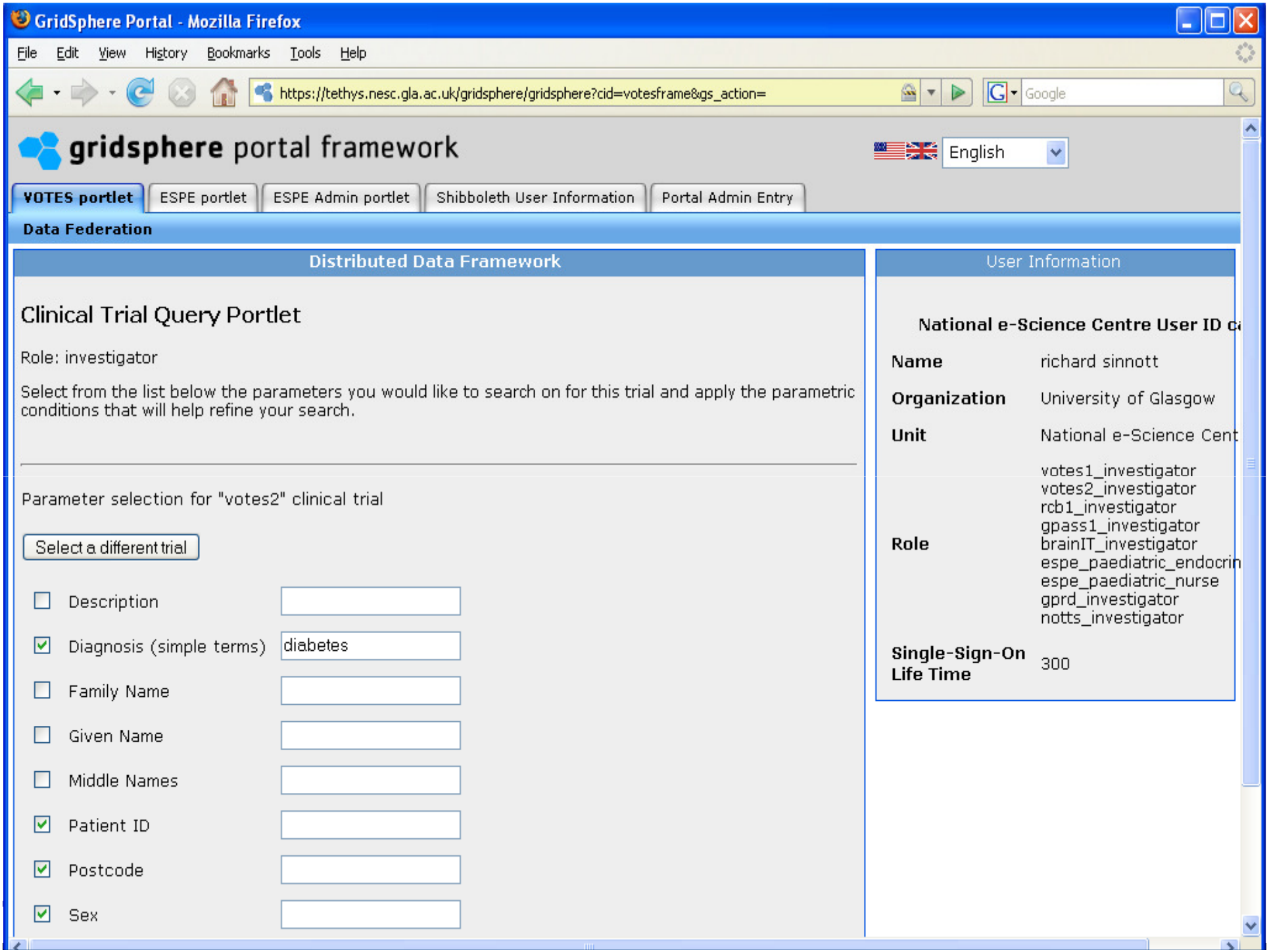
National e-Science Centre User ID card

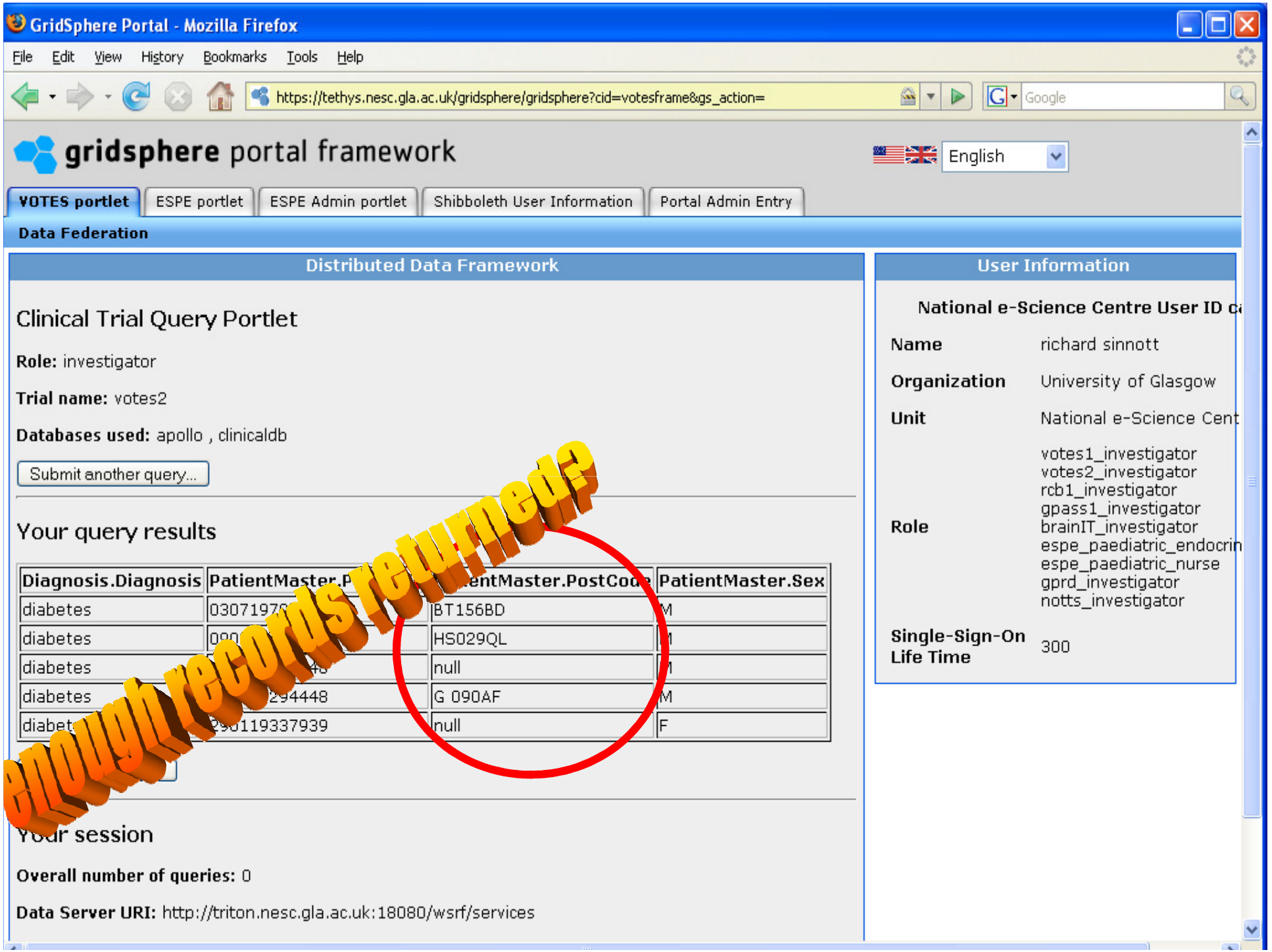
Name	richard [illegible]
Role	votes1_investigator votes2_investigator rcb1_investigator gpass1_investigator brainIT_investigator gemeps_rat_genome_researcher nanoCMOS_deviceModeller nanoCMOS_systemCircuit nanoCMOS_auroraLicense nanoCMOS_taurusLicense espe_paediatric_endocrinologist espe_paediatric_nurse
Organization	University of Glasgow
Unit	National e-Science Centre
Single-Sign-On Life Time	300

powered by gridsphere


GridSphere Portal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tethys.nesc.gla.ac.uk/gridsphere/gridsphere?cid=userinforportlet
Google
gridsphere portal framework
English
VOTES portlet
ESPE portlet
ESPE Admin portlet
Shibboleth User Information
Portal Admin Entry
Shibboleth Attributes
A Shibboleth Attributes Portlet
All Attributes from Shibboleth Identity Provider:
Shib-NameIdentifier-Format
Shib-Person-commonName
richard sinnott
Shib-OrgPerson-orgUnit
Max-Forwards
Shib-TargetedID
Shib-Attributes
Shib-Origin-Site
accept-language
host
Keep-Alive
user-agent
Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.1) Gecko/20061204 Firefox/2.0.0.1
Shib-EP-Affiliation
attributeCertificateAttribute
accept
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
accept-encoding
gzip,deflate
Shib-InetOrgPerson-mail
r.sinnott@nesc.gla.ac.uk
Shib-Authentication-Method
urn:oasis:names:tc:SAML:1.0:am:unspecified
referer
https://tethys.nesc.gla.ac.uk/gridsphere/gridsphere?cid=votesframe&gs_action=
connection
keep-alive
Shib-Application-ID
default
accept-charset
ISO-8859-1,utf-8;q=0.7,*;q=0.7
votes1_investigator
votes2_investigator
rcb1_investigator
gpass1_investigator
Richard Sinnott?
Right Role[s]?
All information needed?

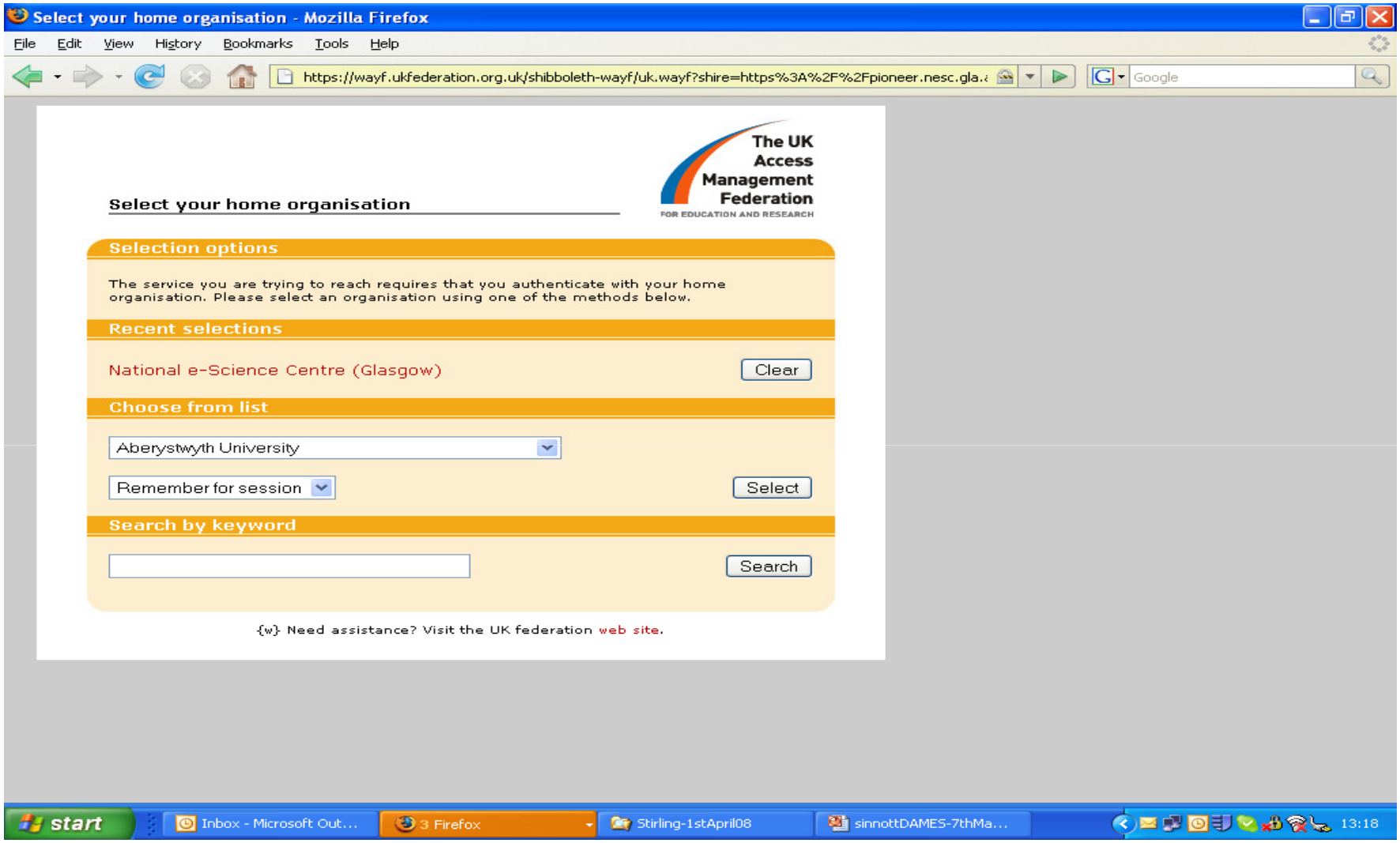

GridSphere Portal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tethys.nesc.gla.ac.uk/gridsphere/gridsphere;jsessionid=03D0C56BFA2201DC36EFC7BAACB800(
Google
gridsphere portal framework
English
VOTES portlet
ESPE portlet
ESPE Admin portlet
Shibboleth User Information
Portal Admin Entry
Data Federation
Clinical Trial Query Portlet
Role: investigator
Select from the list below the parame
the parametric conditions that will he
Parameter selection for "brainIT" cl
Select a different trial
MetaData.CHInum
MetaData.DOB
MetaData.firstName
MetaData.lastName
MetaData.NSH_Initial_Gluco
MetaData.Patient_Image_Det
MetaData.PNSH_GCS_Motc
PatientMaster.CHI
GridSphere Portal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tethys.nesc.gla.ac.uk/gridsphere/gridsphere;jsessionid=66ACB2802AF06E3E5D45680B5135964(
Google
gridsphere portal framework
English
VOTES portlet
ESPE portlet
ESPE Admin portlet
Shibboleth User Information
Portal Admin Entry
Data Federation
Distributed Data Framework
Clinical Trial Query Portlet
Role: nurse
Select from the list below the parameters you would like to search on for this trial and apply the parametric conditions that will help refine your search.
Parameter selection for "brainIT" clinical trial
Select a different trial
MetaData.DOB
PatientMaster.PostCode
PatientMaster.Sex
Submit Query
User Information
National e-Science Centre User
Name
john watt
Role
votes1_nurse
votes2_nurse
brainIT_nurse
gpass1_nurse
gemeps_lymphnodes_genome_
nanoCMOS_taurusLicense
nanoCMOS_systemCircuit
Organization
University of Glasgow
Unit
National e-Science Centre
Single-Sign-On Life Time
300
powered by g

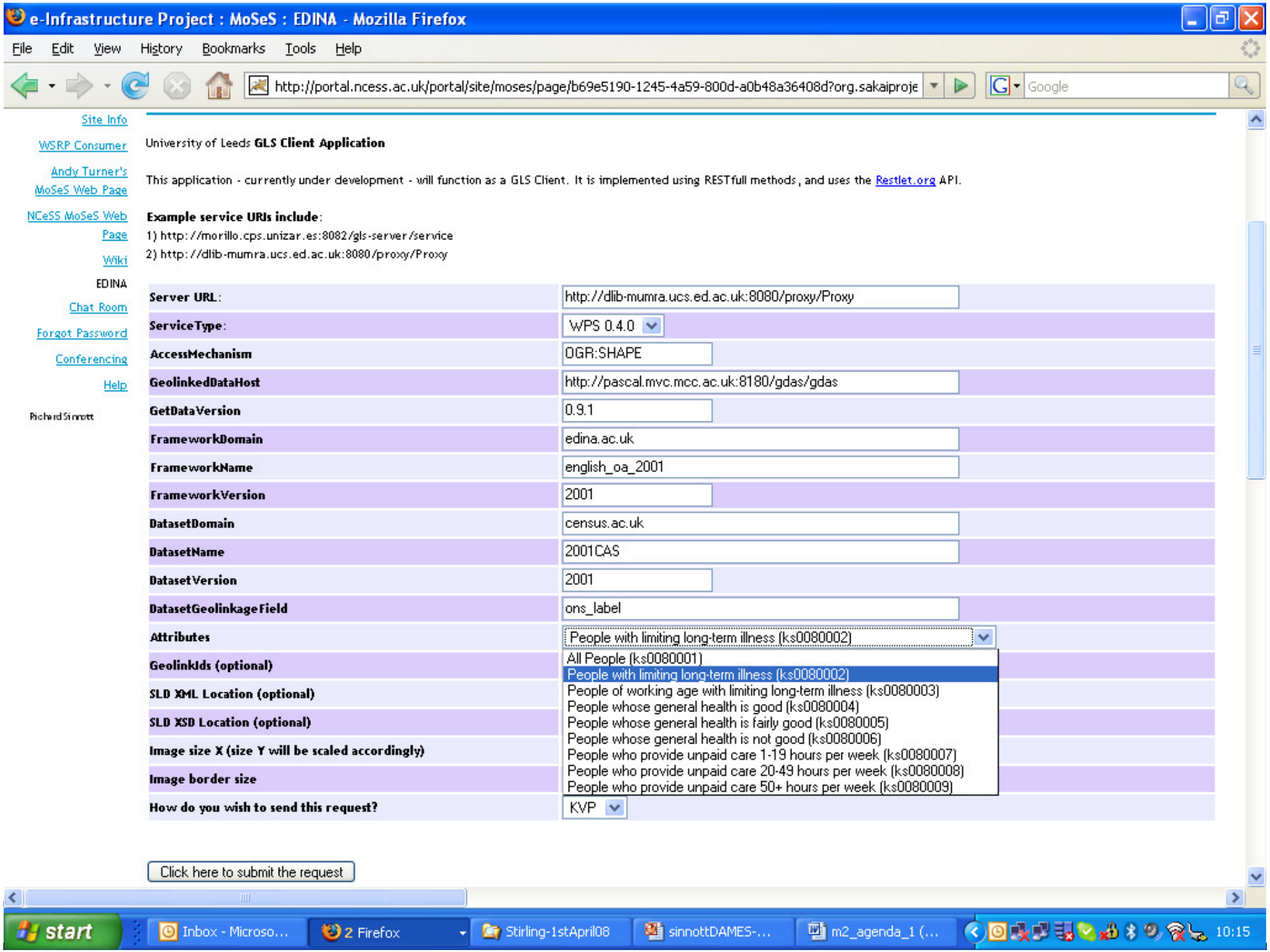

GridSphere Portal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tethys.nesc.gla.ac.uk/gridsphere/gridsphere?cid=votesframe&gs_action=
Google
gridsphere portal framework
English
VOTES portlet
ESPE portlet
ESPE Admin portlet
Shibboleth User Information
Portal Admin Entry
Data Federation
Distributed Data Framework
Clinical Trial Query Portlet
Role: investigator
Select from the list below the parameters you would like to search on for this trial and apply the parametric conditions that will help refine your search.
Parameter selection for "votes2" clinical trial
Select a different trial
Description
Diagnosis (simple terms)
diabetes
Family Name
Given Name
Middle Names
Patient ID
Postcode
Sex
User Information
National e-Science Centre User ID c
Name
richard sinnott
Organization
University of Glasgow
Unit
National e-Science Cent
Role
votes1_investigator
votes2_investigator
rcb1_investigator
gpass1_investigator
brainIT_investigator
espe_paediatric_endocrin
espe_paediatric_nurse
gprd_investigator
notts_investigator
Single-Sign-On Life Time
300

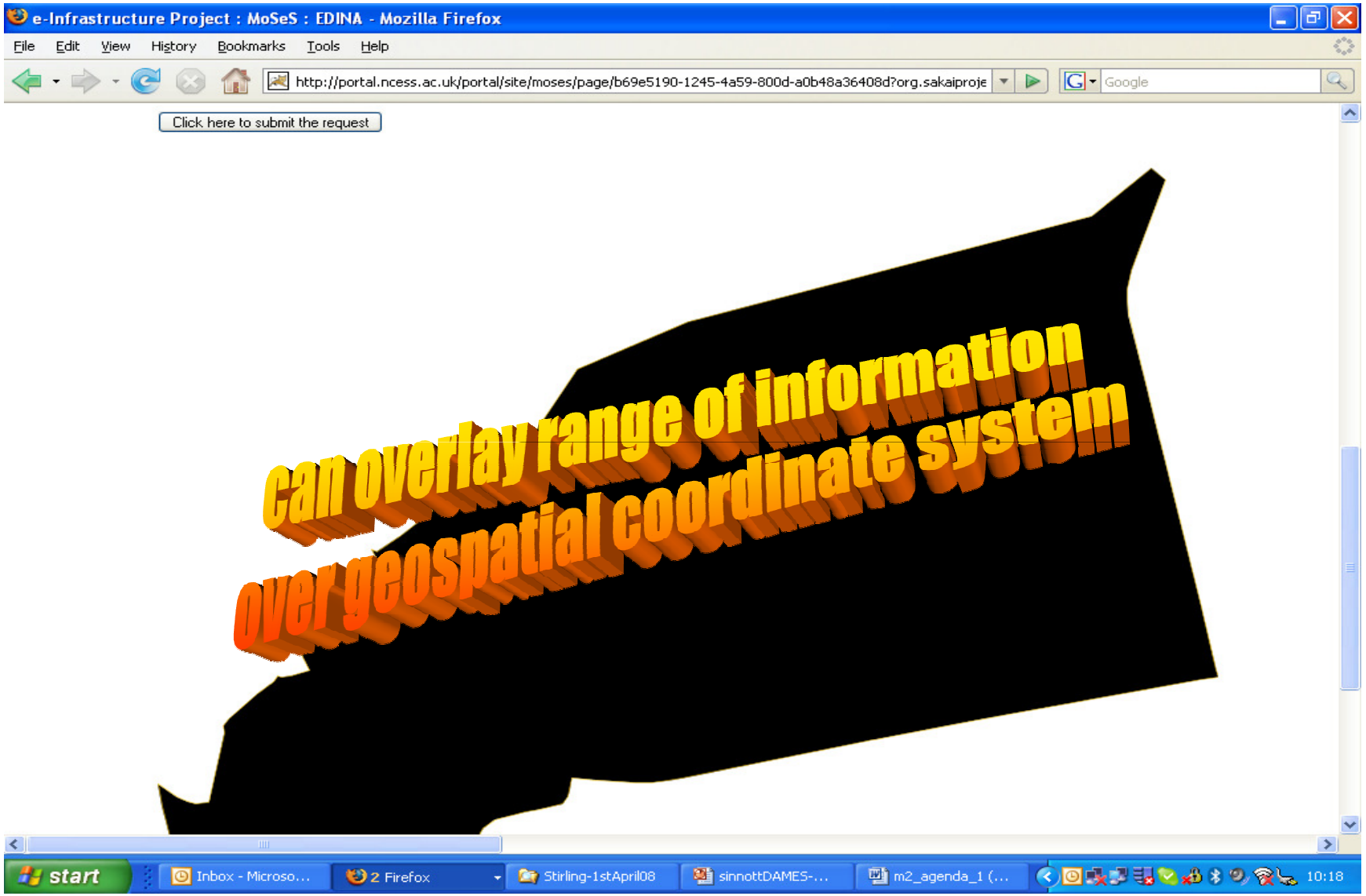

GridSphere Portal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tethys.nesc.gla.ac.uk/gridsphere/gridsphere?cid=votesframe&gs_action=
Google
gridsphere portal framework
English
VOTES portlet
ESPE portlet
ESPE Admin portlet
Shibboleth User Information
Portal Admin Entry
Data Federation
Distributed Data Framework
Clinical Trial Query Portlet
Role: investigator
Trial name: votes2
Databases used: apollo , clinicaldb
Submit another query...
Your query results
Diagnosis.Diagnosis
PatientMaster.Sex
diabetes
BT156BD
HS029QL
G 090AF
null
Enough records returned?
Your session
Overall number of queries: 0
Data Server URI: http://triton.nesc.gla.ac.uk:18080/wsrf/services
User Information
National e-Science Centre User ID
Name
richard sinnott
Organization
University of Glasgow
Unit
National e-Science Cent
Role
votes1_investigator
votes2_investigator
rcb1_investigator
gpass1_investigator
brainIT_investigator
espe_paediatric_endocrin
espe_paediatric_nurse
gprd_investigator
notts_investigator
Single-Sign-On Life Time
300

National e-Science Centre

User redirects browser to geospatial portal


Select your home organisation - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://wayf.ukfederation.org.uk/shibboleth-wayf/uk.wayf?shire=https%3A%2F%2Fpioneer.nesc.gla.
Google
The UK Access Management Federation
FOR EDUCATION AND RESEARCH
Select your home organisation
Selection options
The service you are trying to reach requires that you authenticate with your home organisation. Please select an organisation using one of the methods below.
Recent selections
National e-Science Centre (Glasgow)
Clear
Choose from list
Aberystwyth University
Remember for session
Select
Search by keyword
Search
{w} Need assistance? Visit the UK federation web site.
start
Inbox - Microsoft Out...
3 Firefox
Stirling-1stApril08
sinnottDAMES-7thMa...
13:18


e-Infrastructure Project : MoSeS : EDINA - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://portal.ncess.ac.uk/portal/site/moses/page/b69e5190-1245-4a59-800d-a0b48a36408d?org.sakaiproje
Google
Site Info
WSRP Consumer
Andy Turner's MoSeS Web Page
NCeSS MoSeS Web Page
Wiki
EDINA
Chat Room
Forgot Password
Conferencing
Help
Richard Sinnott
University of Leeds GLS Client Application
This application - currently under development - will function as a GLS Client. It is implemented using RESTfull methods, and uses the Restlet.org API.
Example service URIs include:
1) http://morillo.cps.unizar.es:8082/gls-server/service
2) http://dlib-mumra.ucs.ed.ac.uk:8080/proxy/Proxy
Server URL: http://dlib-mumra.ucs.ed.ac.uk:8080/proxy/Proxy
ServiceType: WPS 0.4.0
AccessMechanism: OGR:SHAPE
GeolinkedDataHost: http://pascal.mvc.mcc.ac.uk:8180/gdas/gdas
GetDataVersion: 0.9.1
FrameworkDomain: edina.ac.uk
FrameworkName: english_oa_2001
FrameworkVersion: 2001
DatasetDomain: census.ac.uk
DatasetName: 2001CAS
DatasetVersion: 2001
DatasetGeolinkageField: ons_label
Attributes: People with limiting long-term illness (ks0080002)
All People (ks0080001)
People with limiting long-term illness (ks0080002)
People of working age with limiting long-term illness (ks0080003)
People whose general health is good (ks0080004)
People whose general health is fairly good (ks0080005)
People whose general health is not good (ks0080006)
People who provide unpaid care 1-19 hours per week (ks0080007)
People who provide unpaid care 20-49 hours per week (ks0080008)
People who provide unpaid care 50+ hours per week (ks0080009)
GeolinkIds (optional)
SLD XML Location (optional)
SLD XSD Location (optional)
Image size X (size Y will be scaled accordingly)
Image border size
How do you wish to send this request? KVP
Click here to submit the request
start
Inbox - Microso...
2 Firefox
Stirling-1stApril08
sinnottDAMES-...
m2_agenda_1 (...
10:15


e-Infrastructure Project : MoSeS : EDINA - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://portal.ncess.ac.uk/portal/site/moses/page/b69e5190-1245-4a59-800d-a0b48a36408d?org.sakaiproje
Google
Click here to submit the request
can overlay range of information
over geospatial coordinate system
start
Inbox - Microso...
2 Firefox
Stirling-1stApril08
sinnottDAMES-...
m2_agenda_1 (...
10:18

National e-Science Centre

SPAM-GP (the video!)

Conclusions

National e-Science Centre

- Clinical systems driven by Information Governance/Ethics
  - MREC, LREC, PAC, PIAG, Caldicott Guardians, Joe Public
- Once defined have tools/techniques to rapidly roll-out e-Infrastructures to support researchers
  - Diabetes?
  - Cancer?
  - Obesity?
  - Smoking?
  - Health/Wealth?
  - Genetics and Healthcare?
  - Nature / Nurture?
- Focus not on single VO but supporting many VOs that have their own access/usage policies

Next Steps

National e-Science Centre

- Scottish Health Informatics Platform
  - 3 year project £3.6m funded by Wellcome Trust, EPSRC, ESRC, MRC
  - Starts January 2009
  - ~£1m for NHS to work with us
- Secure Access to Scottish Morbidity Records, other data sets
  - GridSphere portal exploiting SPAM-GP
- Completion of SeeGEO demonstrator
  - MIMAS Census data
  - EDINA UK Borders data
- Working with UK Data Archives / CESSDA PPP
  - e-possibilities and roadmap

National e-Science Centre

Questions ...?