How Grid Security works in GEO Sciences

N. Yamamoto, Y. Tanaka, I. Kojima, S. Sekiguchi
AIST

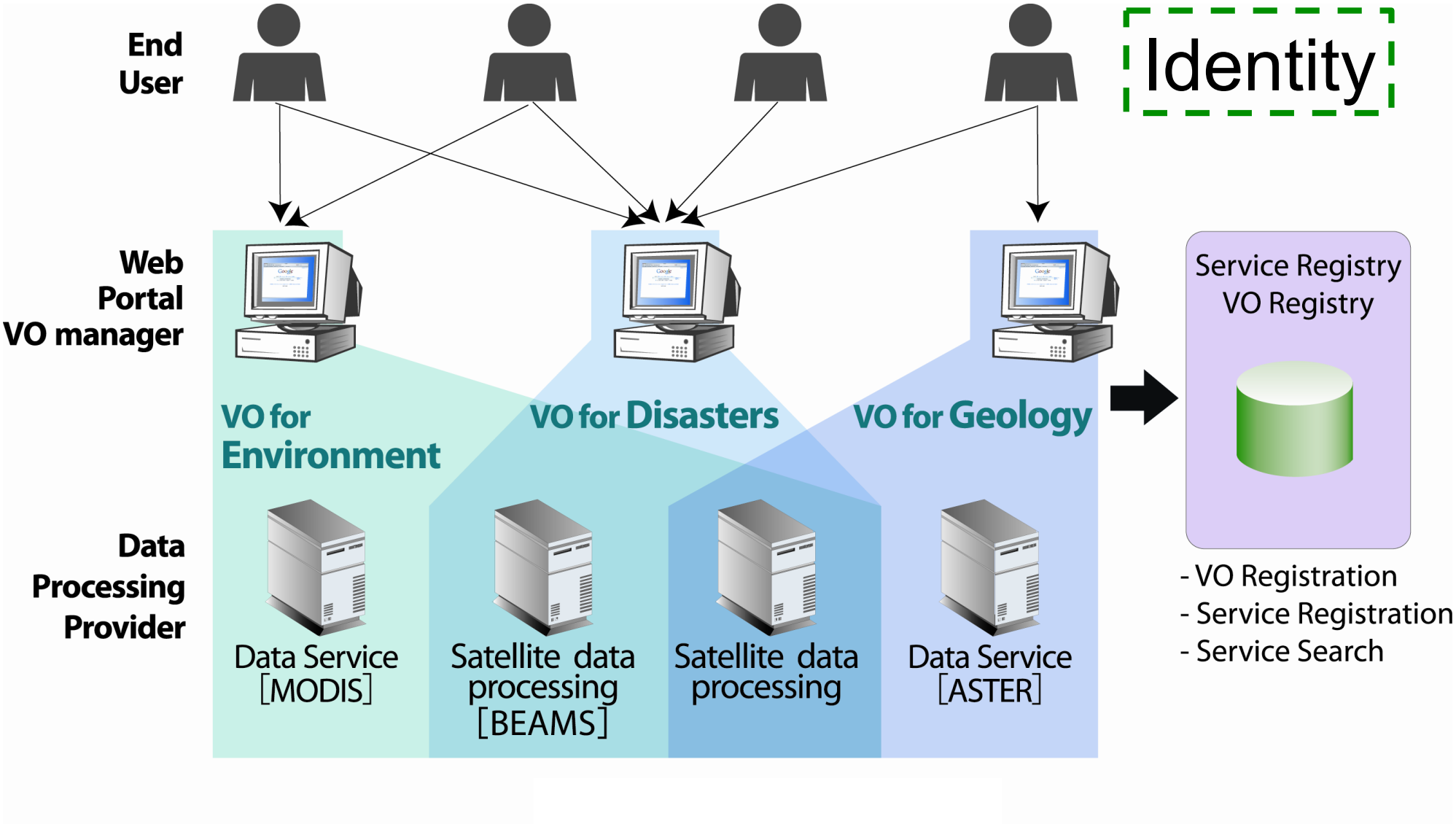
Oct. 28, 2009 GEO Workshop / PRAGMA17
Hanoi

GEOGrid
http://www.geogrid.org/

What is Grid Security

- Who am I? / Who are they?
  - Grid Security Infrastructure (GSI)
- What can I do? / What can they do?
  - Virtual Organization Membership Service (VOMS)

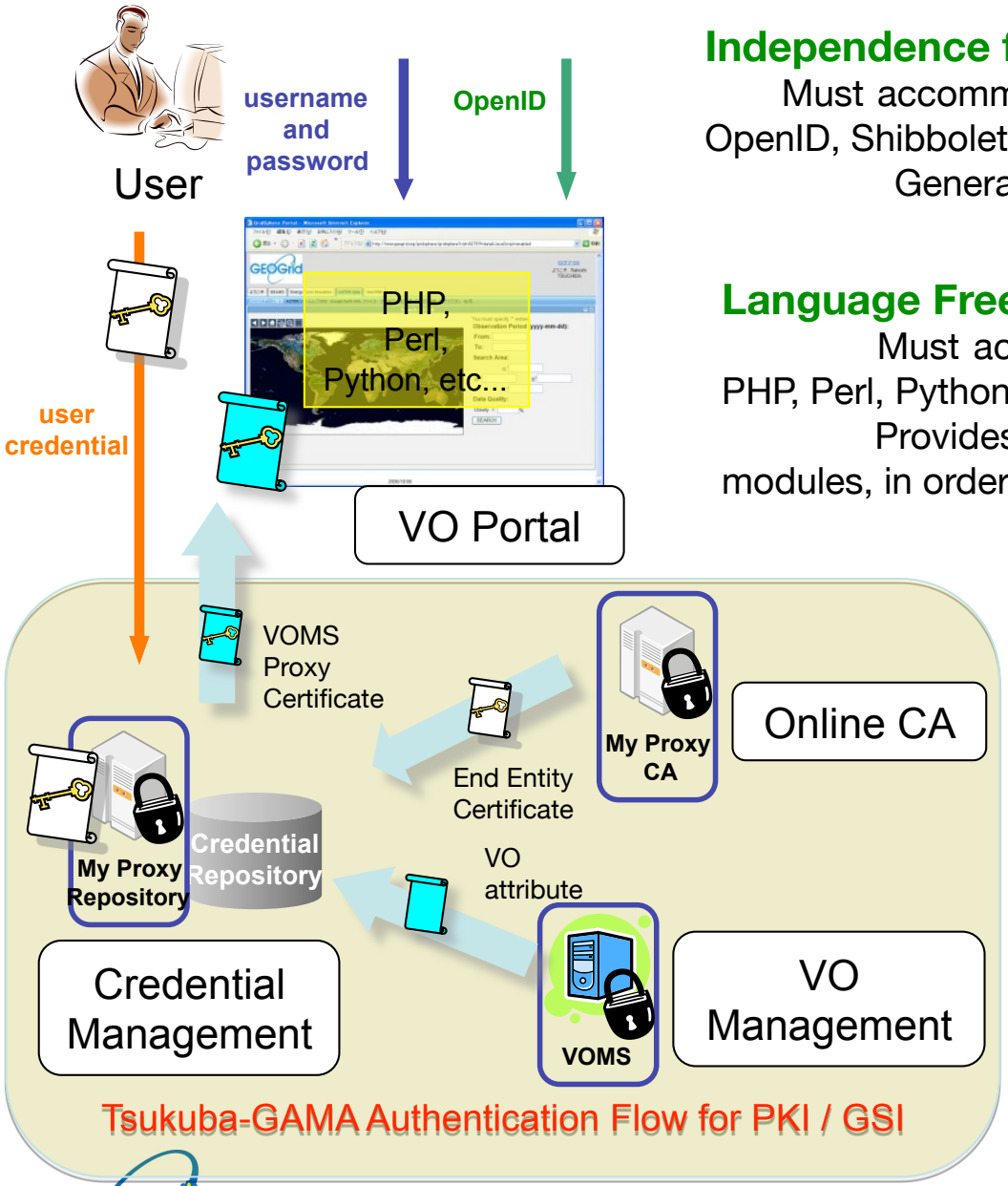
GEO Grid VO Design



Requirements

- Credential Management:
  - Non-secure users often manage their private keys for PKI / GSI credentials without careful planning.
- Authentication methods:
  - Must accommodate existing, settled authentication methods, OpenID, Shibboleth, username and password, user credential, etc.
- Portal Development:
  - Must accommodate existing application portals written by PHP, Perl, Python, Java Servlet, etc.

OUR SOLUTION: TSUKUBA-GAMA



Independence from Authentication methods:

Must accommodate existing, settled authentication methods, OpenID, Shibboleth, username and password, user credential, etc.
Generates Grid credentials from any method.

Language Free Portal Development:

Must accommodate existing application portals written by PHP, Perl, Python, Java Servlet, etc.

Provides Apache, Servlet, and GridSphere authentication modules, in order to support any language.

Credential Management:

Non-secure users often manage their private keys for PKI / GSI without careful planning.

Manages user credentials on the server side, instead of leaving it to inexperienced users.

DEMO 1:
TSUKUBA-GAMA
LOGIN PRAGMA VO PORTAL
(GRIDSPHERE)

Demo Environments - login

USER

1. input username and pass of user cert

PRAGMA VO portal
http://gfm49.apgrid.org/gridsphere/

voms
proxy cert

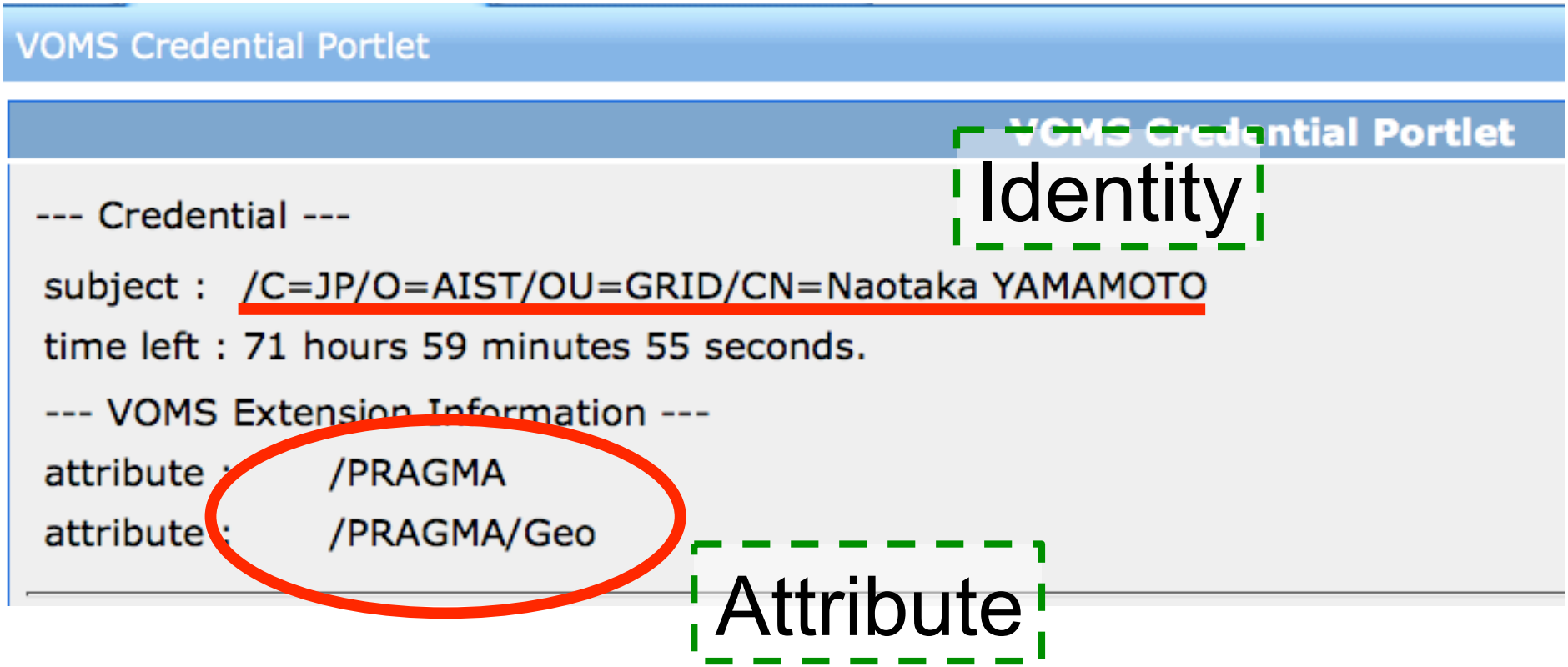
4. register proxy cert

Credential
Repository

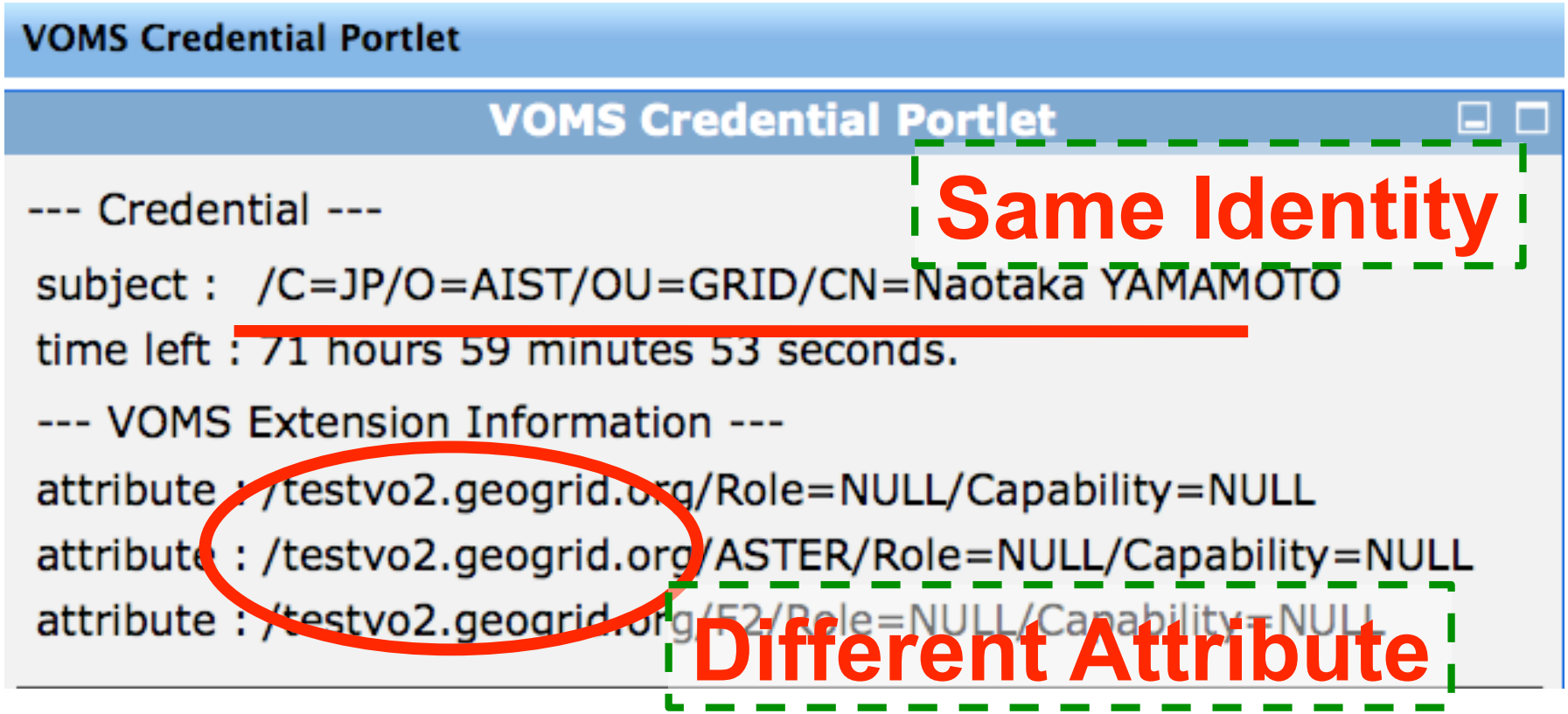
2. generate gloubs
proxy certificate

PRAGMA VOMS

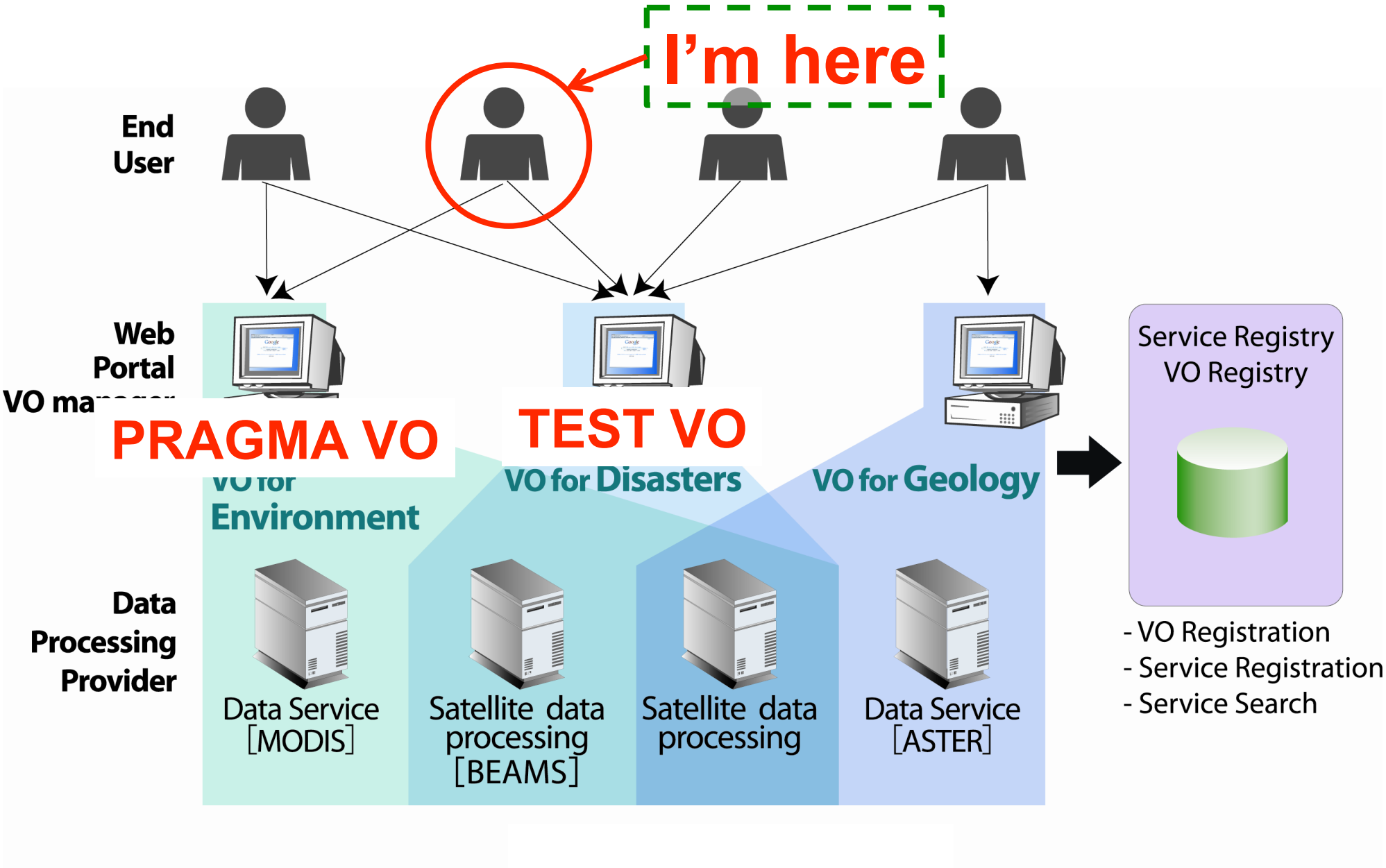
3. add voms attribute


VOMS Credential Portlet
VOMS Credential Portlet
Identity
--- Credential ---
subject : /C=JP/O=AIST/OU=GRID/CN=Naotaka YAMAMOTO
time left : 71 hours 59 minutes 55 seconds.
--- VOMS Extension Information ---
attribute : /PRAGMA
attribute : /PRAGMA/Geo
Attribute

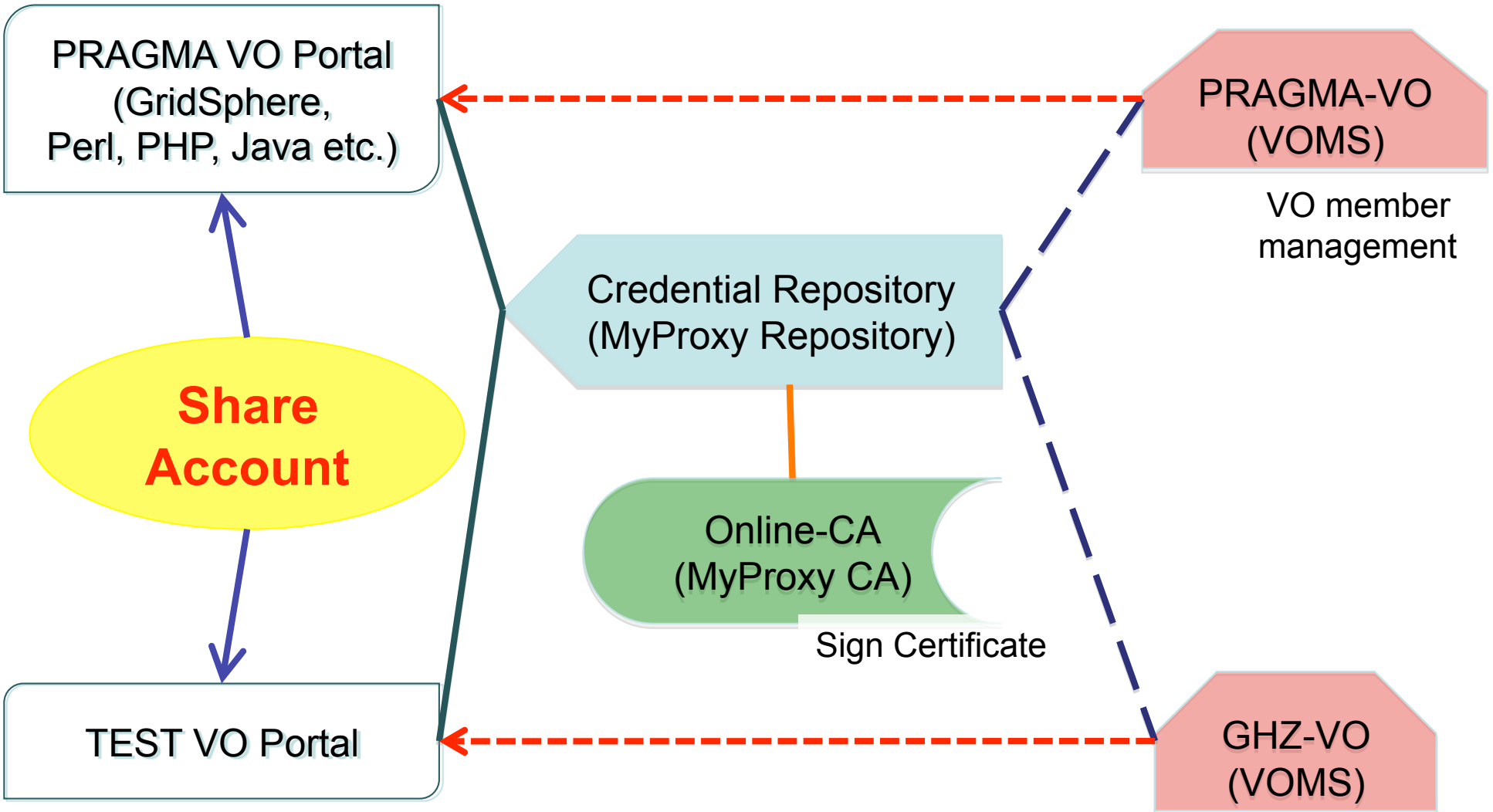
DEMO 2: TSUKUBA-GAMA LOGIN TESTVO PORTAL (GRIDSPHERE)


VOMS Credential Portlet
VOMS Credential Portlet
--- Credential ---
subject : /C=JP/O=AIST/OU=GRID/CN=Naotaka YAMAMOTO
time left : 71 hours 59 minutes 53 seconds.
--- VOMS Extension Information ---
attribute : /testvo2.geogrid.org/Role=NULL/Capability=NULL
attribute : /testvo2.geogrid.org/ASTER/Role=NULL/Capability=NULL
attribute : /testvo2.geogrid.org/F2/Role=NULL/Capability=NULL
Same Identity
Different Attribute

GEO Grid VO Design

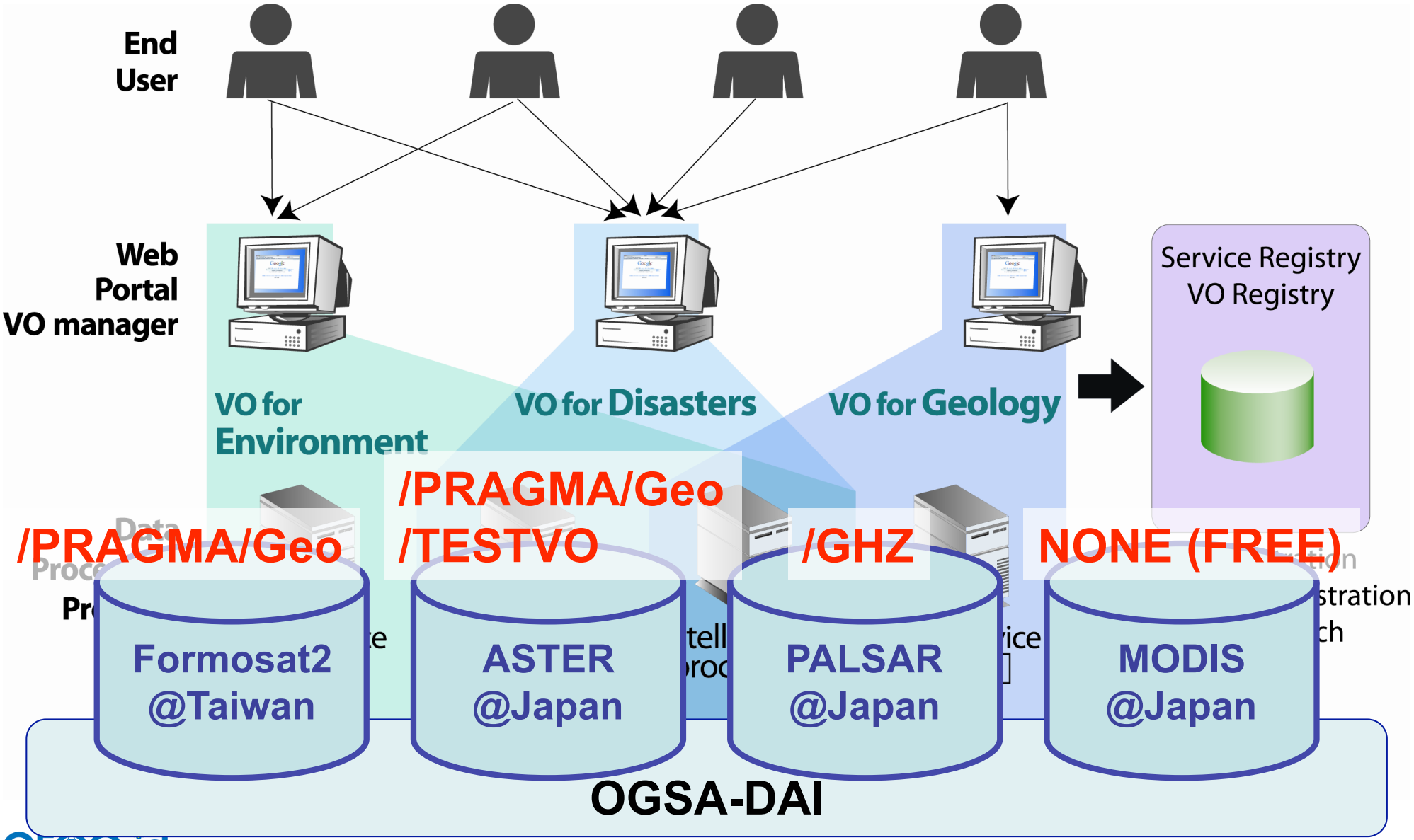


GSI w/ VOMS

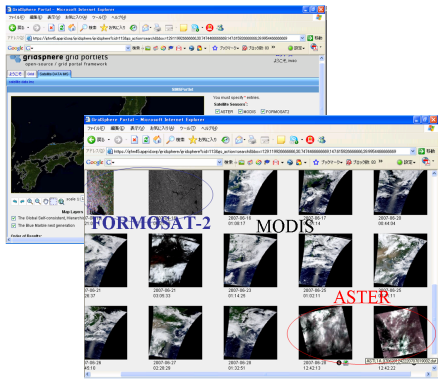

PRAGMA VO Portal
(GridSphere,
Perl, PHP, Java etc.)
PRAGMA-VO
(VOMS)
VO member
management
Credential Repository
(MyProxy Repository)
Share
Account
Online-CA
(MyProxy CA)
Sign Certificate
TEST VO Portal
GHZ-VO
(VOMS)

EXAMPLE SCENARIO: SATELLITE DATABASE FEDERATION

Demo environment



DEMO 3: SIMS SATELLITE DATABASE FEDERATION



Java Program

Integration Framework with OGSA-DAI

OGSA-DAI Client

SQL

SQL

SQL

SQL

SQL

SIMS portlet
- **query data**
- **create web page which shows thumbnail images**

Application Server

Globus

OGSA-DAI

VOMS

SQL w/ JDBC

Database Server (Sybase)

FORMOSAT-2

VOMS

Globus

OGSA-DAI

OGSA-DAI

SQL w/ JDBC

Database Server (PostgreSQL)

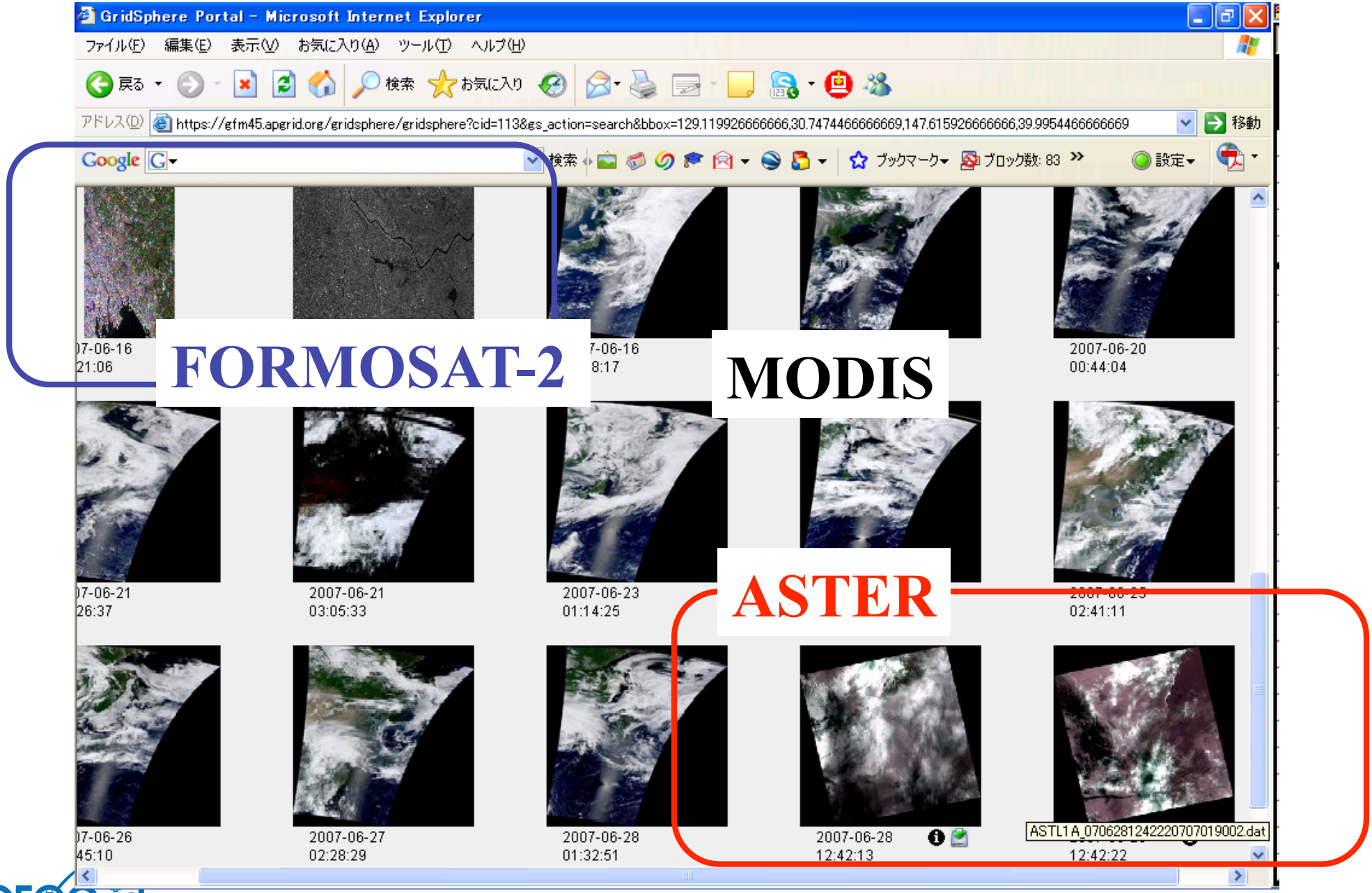
ASTER

MODIS

NSPO@TW AIST@JP

SIMS – Search Results

http://www.geogrid.org

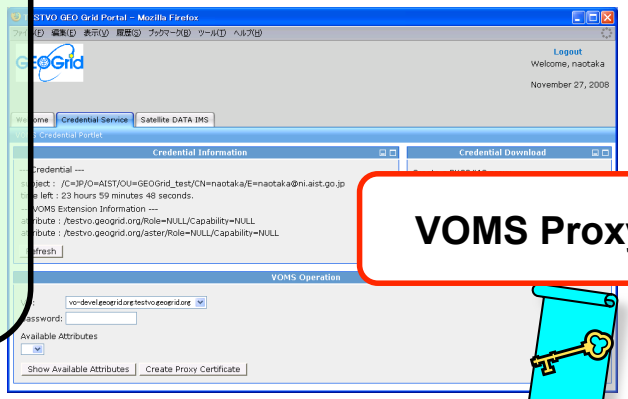


DEMO 4: LANGUAGE FREE PORTAL DEVELOPMENT

DEMO 4-1: PORTAL DEVELOPMENT (OPENLAYERS)

User

OGCProxy



https://portal/OGCProxy?\
URL=https://gridsite/..../service

GridSite

Powered by APACHE

ACL:
/testvo.geogrid.org/aster
VO Name Group

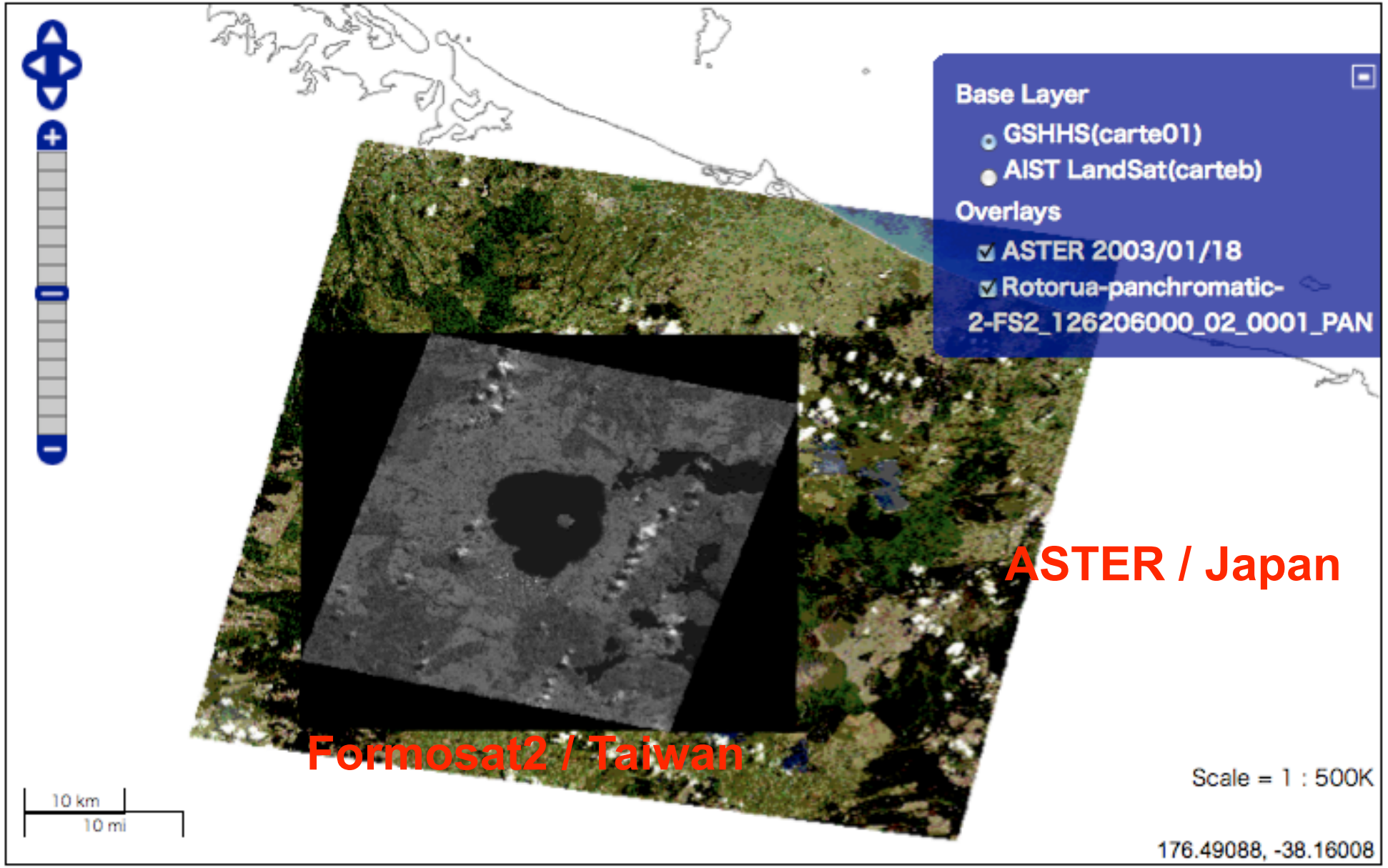
Contents

https://gridsite/..../service

- OGCProxy is a broker portlet
  - forwarding users' requests to backend OGC services.
  - providing freely development environment of client application.

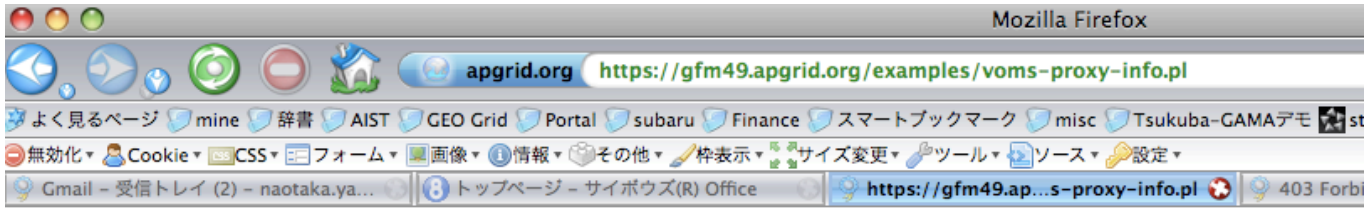
ASTER + Formosat2 / OpenLayers

http://www.geogrid.org



DEMO 4-2: PORTAL DEVELOPMENT (PHP, PERL, ...)

- apache_ahtn_myproxy module
  - PHP, Perl, Phython, etc.
- Servlet basic authentication module
  - Java Servlet
- GridSphere authentication module



voms-proxy-info

```
subject   : /C=JP/O=AIST/OU=GRID/CN=Naotaka YAMAMOTO/CN=742169096/CN=1413599050/CN=1607894758/CN=1607894758
issuer    : /C=JP/O=AIST/OU=GRID/CN=Naotaka YAMAMOTO/CN=742169096/CN=1413599050/CN=1607894758
identity  : /C=JP/O=AIST/OU=GRID/CN=Naotaka YAMAMOTO/CN=742169096/CN=1413599050/CN=1607894758
type      : RFC compliant proxy
strength  : 1024 bits
path      : /srv/www/cert/f86cd36b536383c80103fc9a83a778a43b3c2932-delegation
timeleft  : 28:32:28
=== VO PRAGMA extension information ===
VO        : PRAGMA
subject   : /C=JP/O=AIST/OU=GRID/CN=Naotaka YAMAMOTO
issuer    : /DC=NET/DC=PRAGMA-GRID/OU=SDSC/CN=vomrs-pragma.sdsc.edu
attribute : /PRAGMA
attribute : /PRAGMA/Geo
timeleft  : 28:32:30
uri       : vomrs-pragma.sdsc.edu:15001
```

DEMO 5: INDEPENDENCE FROM AUTHENTICATION METHODS

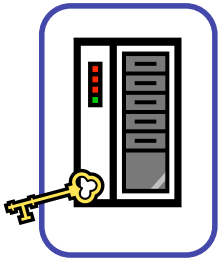
DEMO 5-1: INDEPENDENCE FROM AUTHENTICATION METHODS: (OPENID)

OpenID authentication module

http://www.geogrid.org

User

Password for OpenID

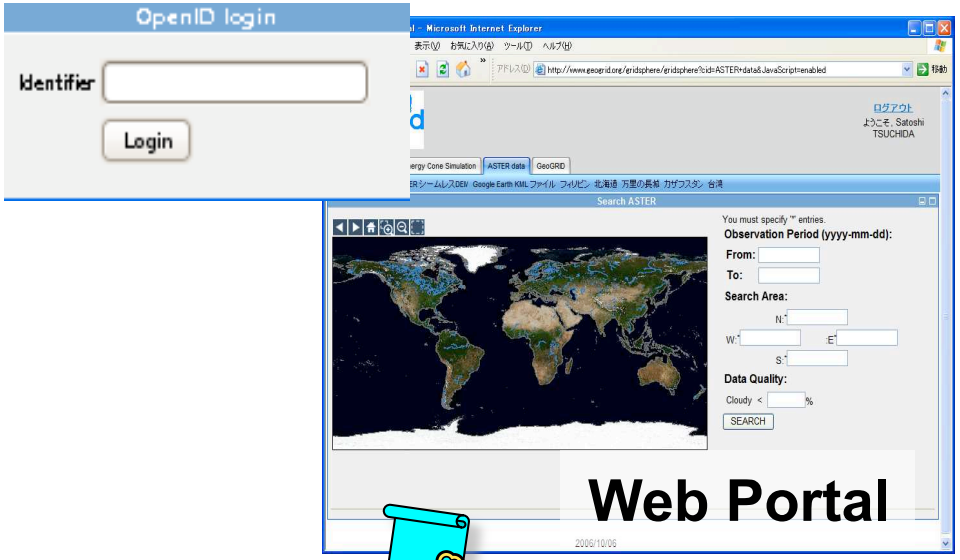


OpenID Server

MyProxy CA

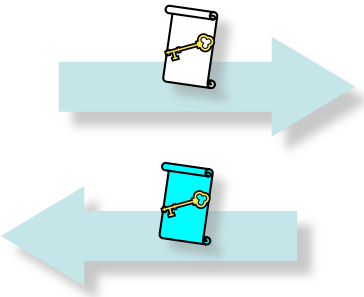
OpenID URL

Request short-lived credential



Web Portal

- Account DB
- Credential Repository



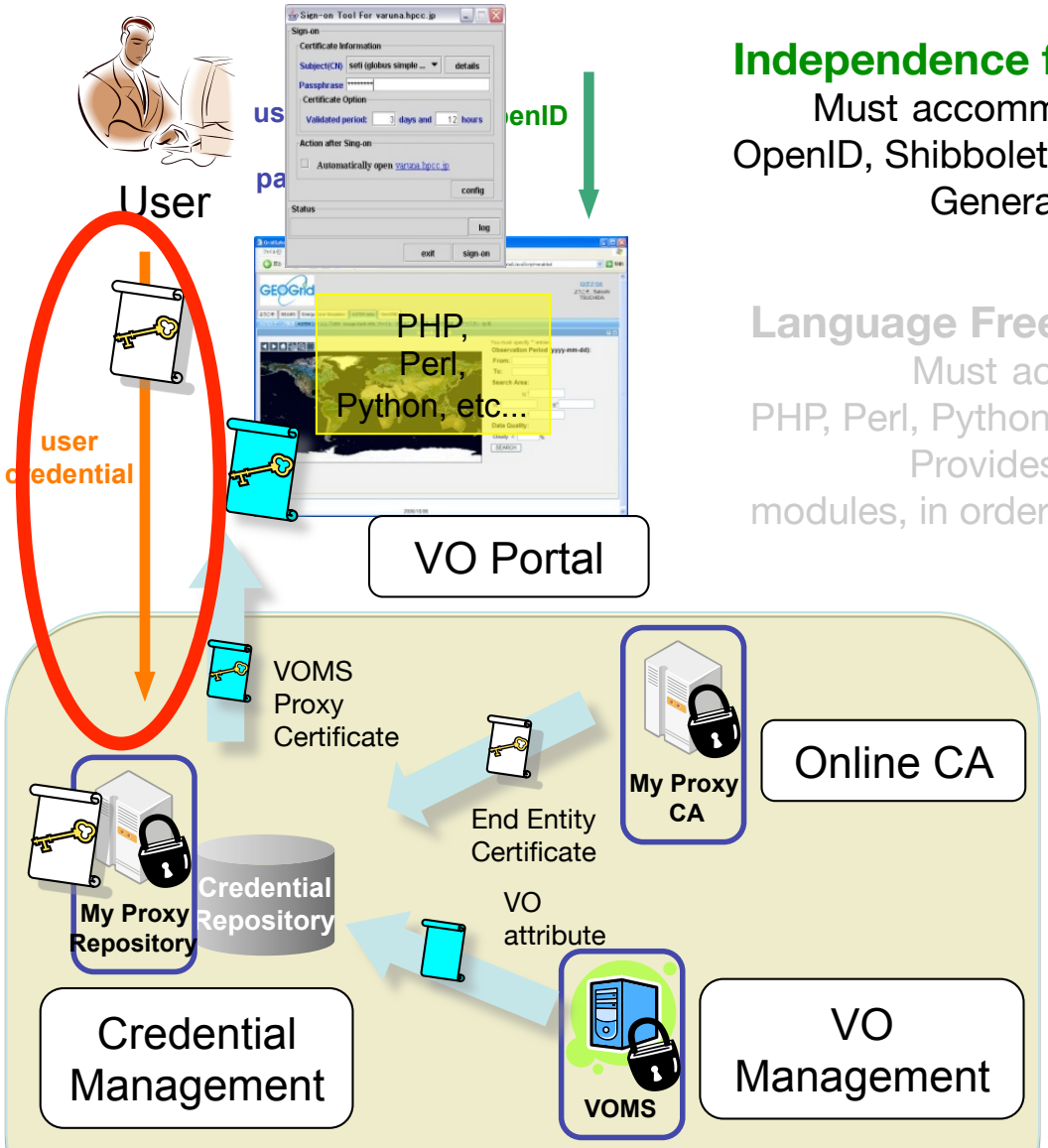
VOMS proxy

VO member DB

VOMS server

DEMO 5-1: INDEPENDENCE FROM AUTHENTICATION METHODS: (CREDENTIAL)

Credential Login



Independence from Authentication methods:

Must accommodate existing, settled authentication methods, OpenID, Shibboleth, username and password, user credential, etc.
Generates Grid credentials from any method.

Language Free Portal Development:

Must accommodate existing application portals written by PHP, Perl, Python, Java Servlet, etc.

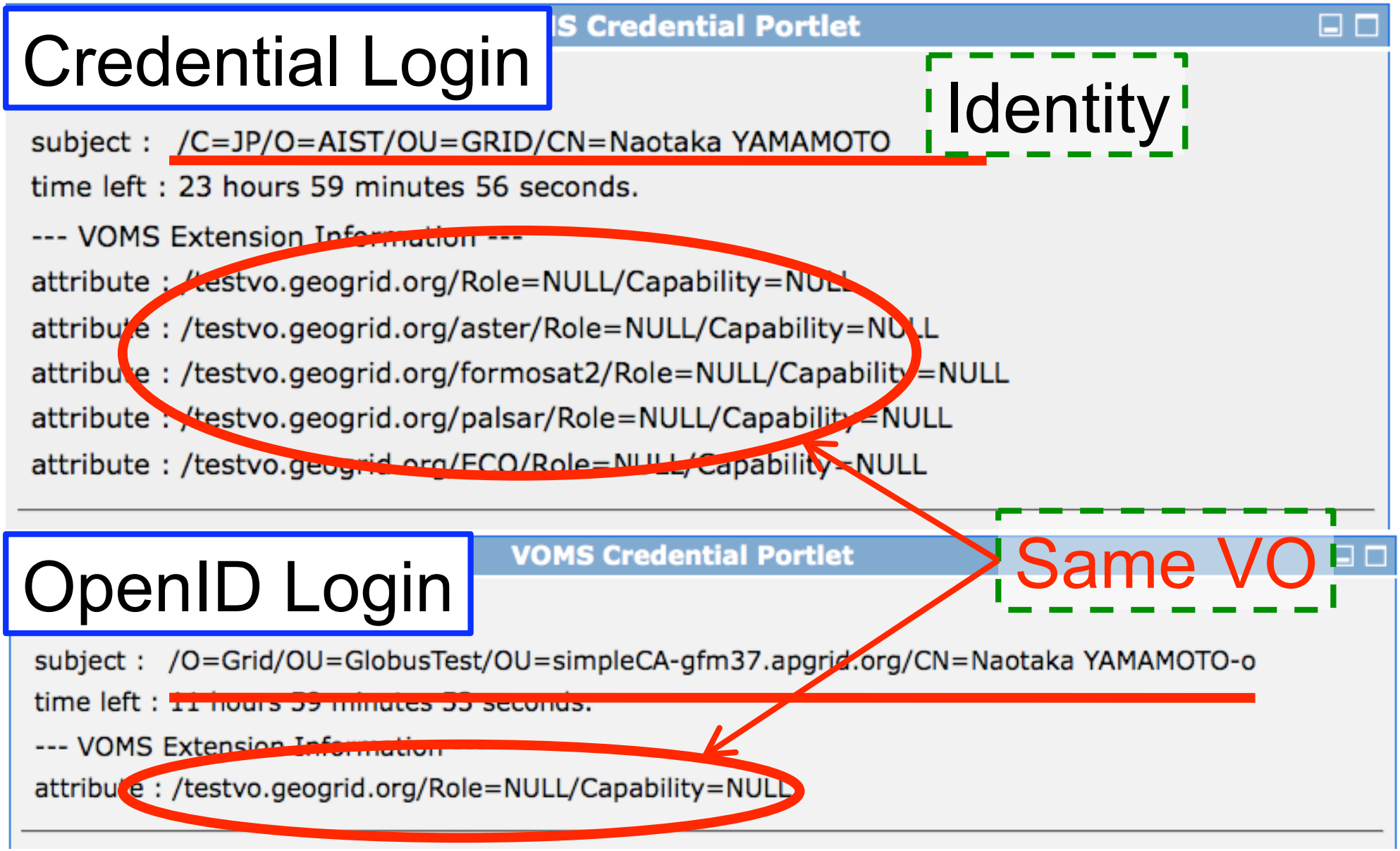
Provides Apache, Servlet, and GridSphere authentication modules, in order to support any language.

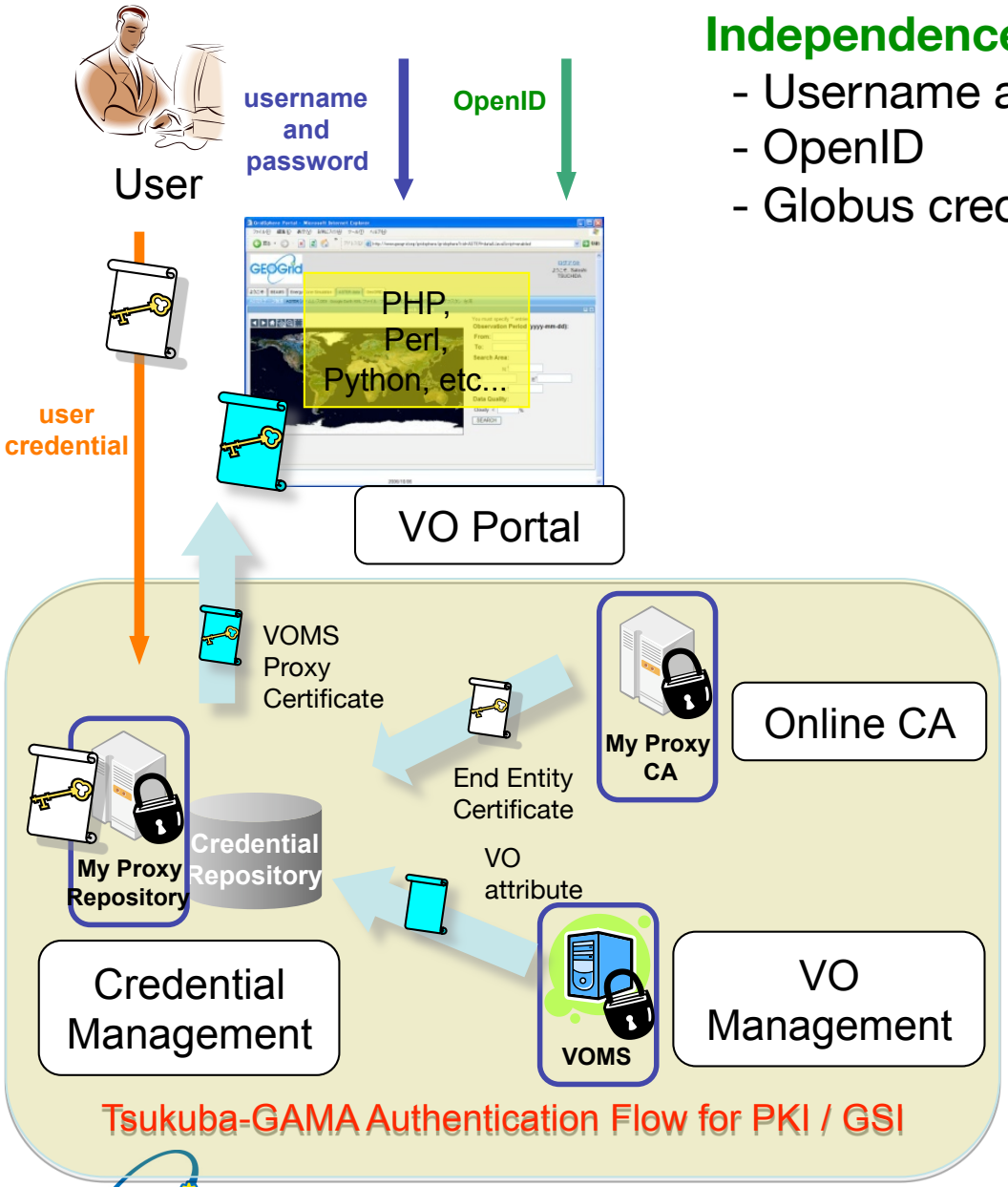
Credential Management:

Non-secure users often manage their private keys for PKI / GSI without careful planning.

Manages user credentials on the server side, instead of leaving it to inexperienced users.

Compare Identity





Independence from Authentication methods:

- Username and Password
- OpenID
- Globus credential

Language Free Portal Development:

- GridSphere / Satellite database federation
- Geographical portal / OpenLayers
- PHP, Perl

Credential Management:

- User does not need to manage their credentials

THANK YOU

To be released NEXT month!