

SHEBANGS

Shibboleth Enabled Bridge to Access the National Grid Service

Mike Jones

Aleksandra Nenadic, Stephen Pickles, Ning Zhang

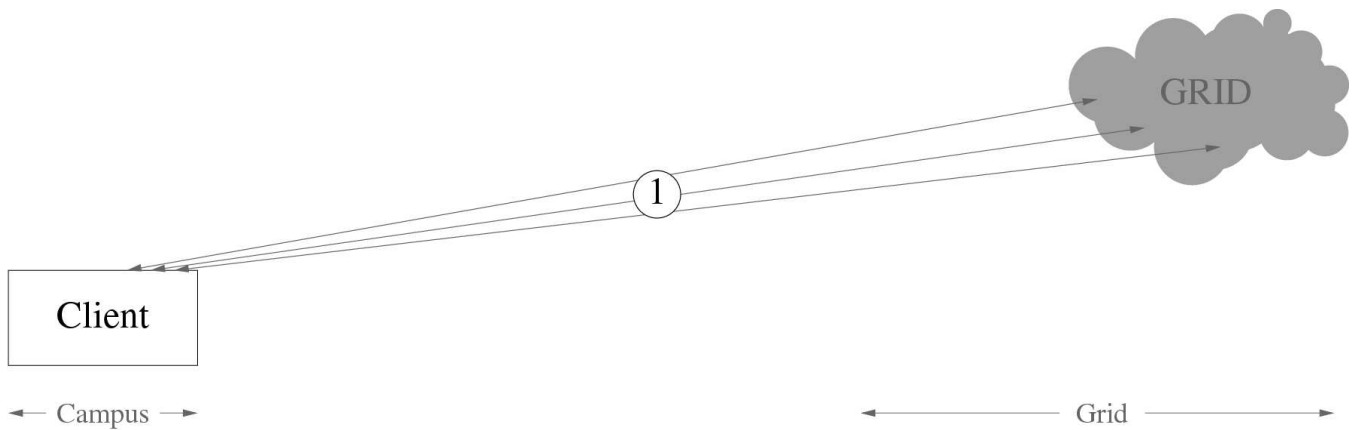
Grid and Shib ad hoc BOF, GGF16

Basic Access to the National Grid Service Today

NGS is a Globus 2 based Grid

- Users need the means to authenticate themselves: GSI credentials
- The NGS needs the means to make authorization decisions: Grid-map +...
- Users need heavyweight tools and network access

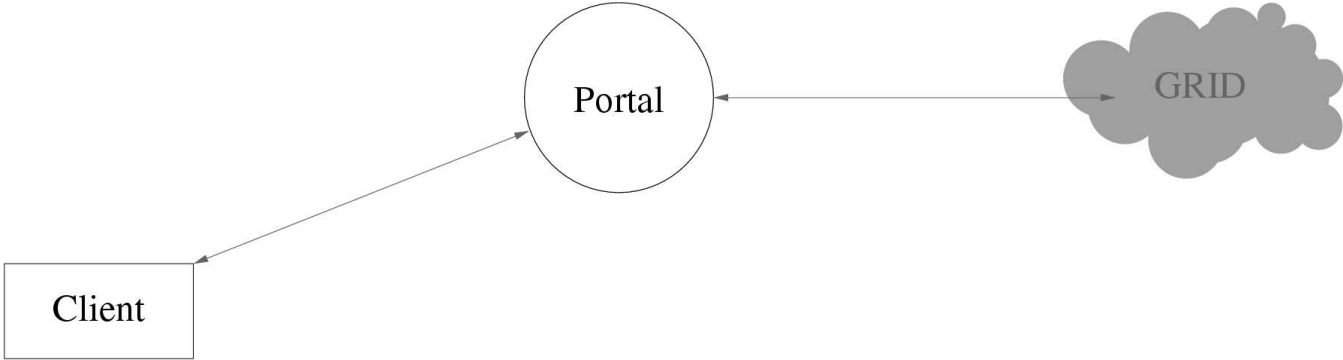
We target users without these.



Combining the strengths of UMIST and
The Victoria University of Manchester

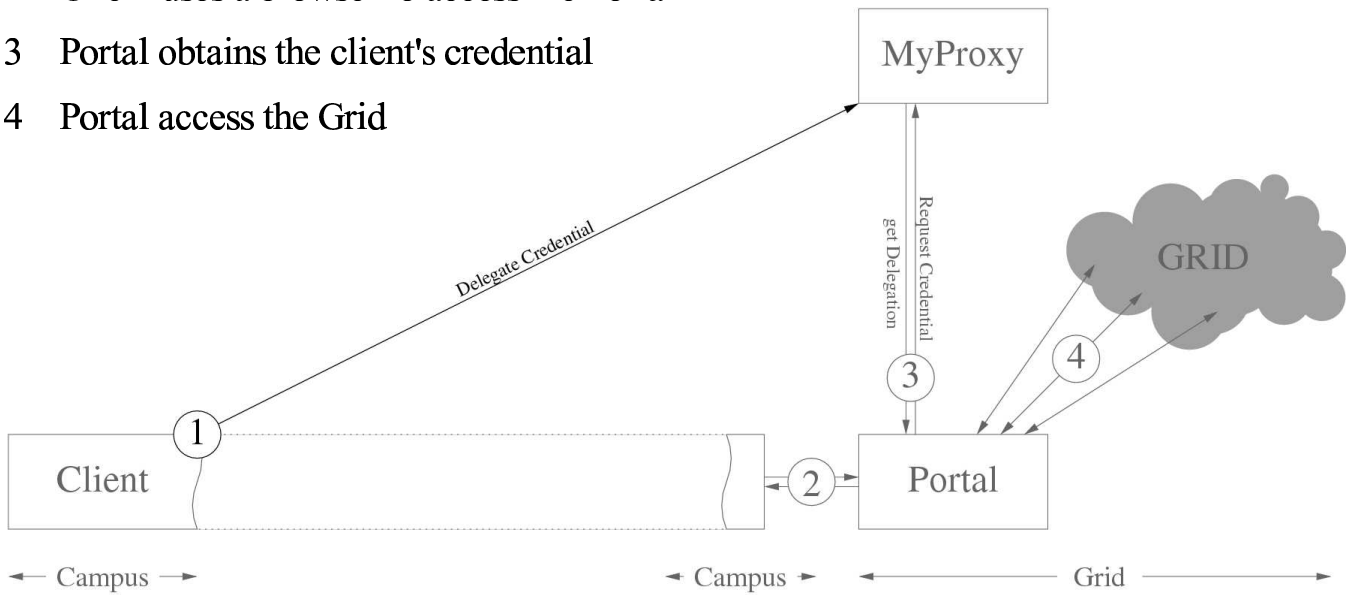
Portal Access to the National Grid Service Today

- Clients no longer need heavyweight tools.



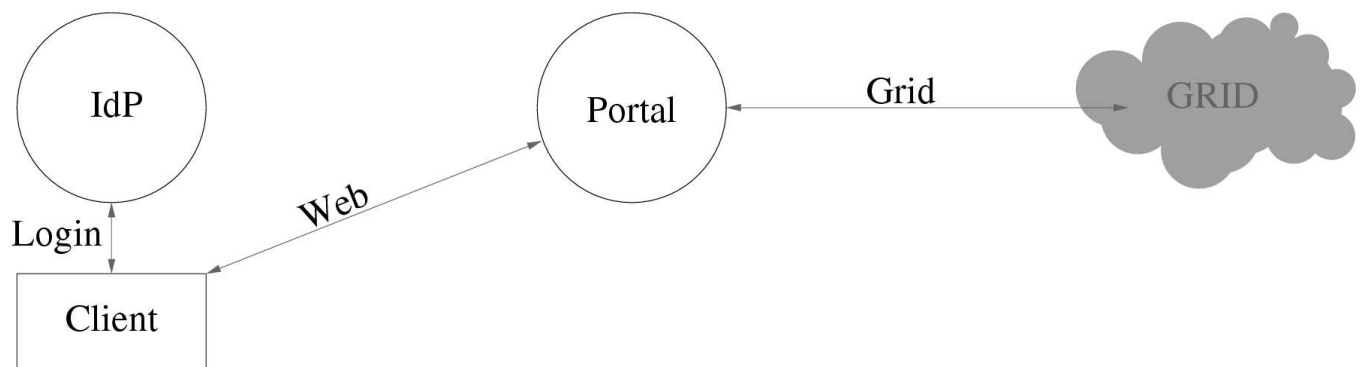
Portal Access to the National Grid Service Today

- 1 Client delegates their credential to MyProxy
- 2 Client uses a browser to access the Portal
- 3 Portal obtains the client's credential
- 4 Portal access the Grid

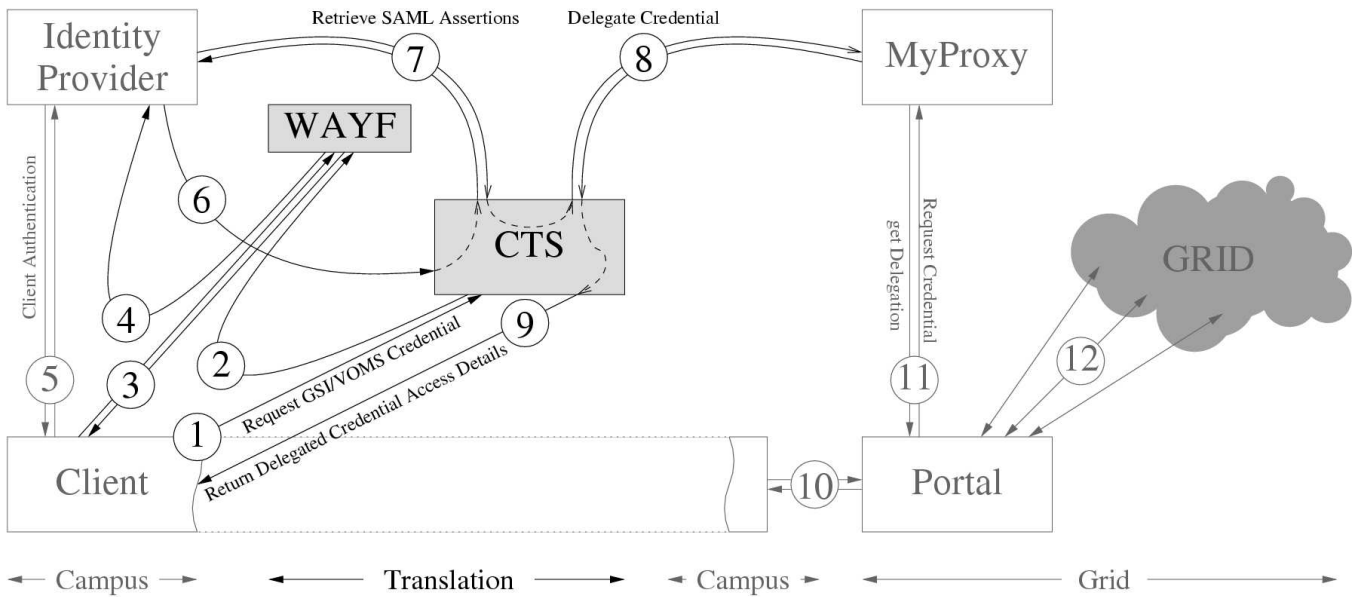


Portal Access to the NGS through SHEBANGS

- Clients no longer need heavyweight tools.
- Clients no longer need GSI Credentials



Shibboleth Bridge to the National Grid Service



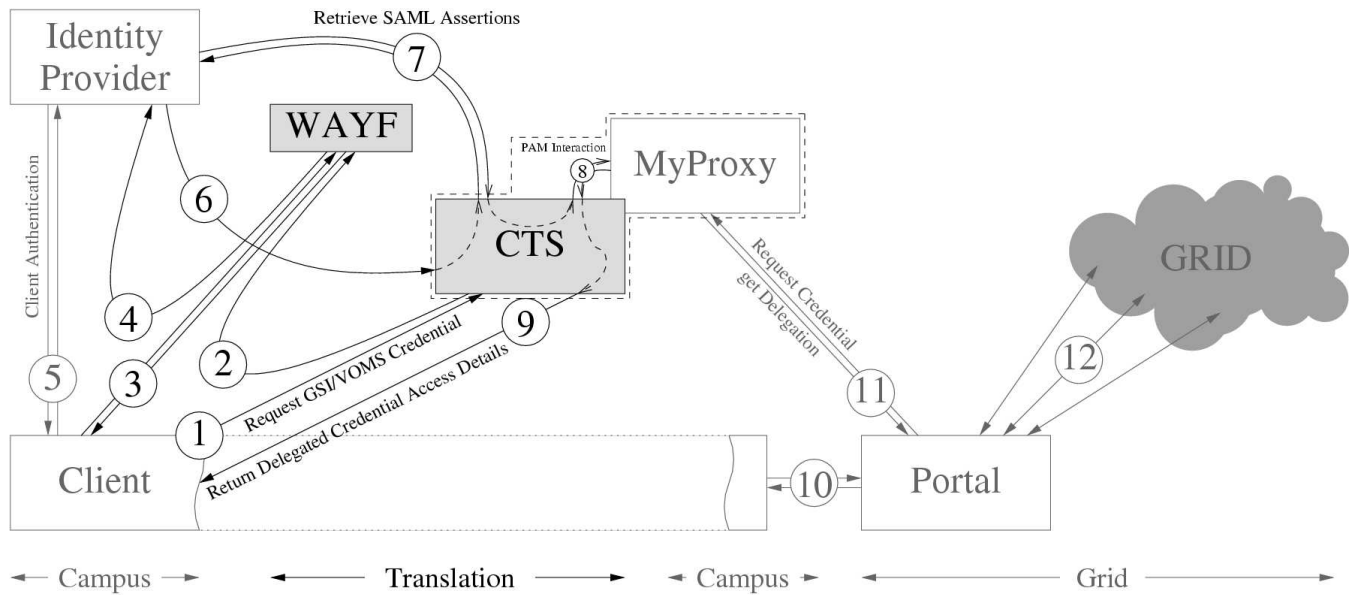
Combining the strengths of UMIST and
The Victoria University of Manchester

Portal Access to the NGS through SHEBANGS

- Issues
 - The system covers only authentication
 - The identity credentials will be authentic
 - Authorization step remains incomplete
 - Need/want to use VOMS attributes
- Outcomes
 - Clients no longer need GSI Credentials of their own.
 - Credential Translation Service
 - Shibbolized VOMS service
 - Online CA

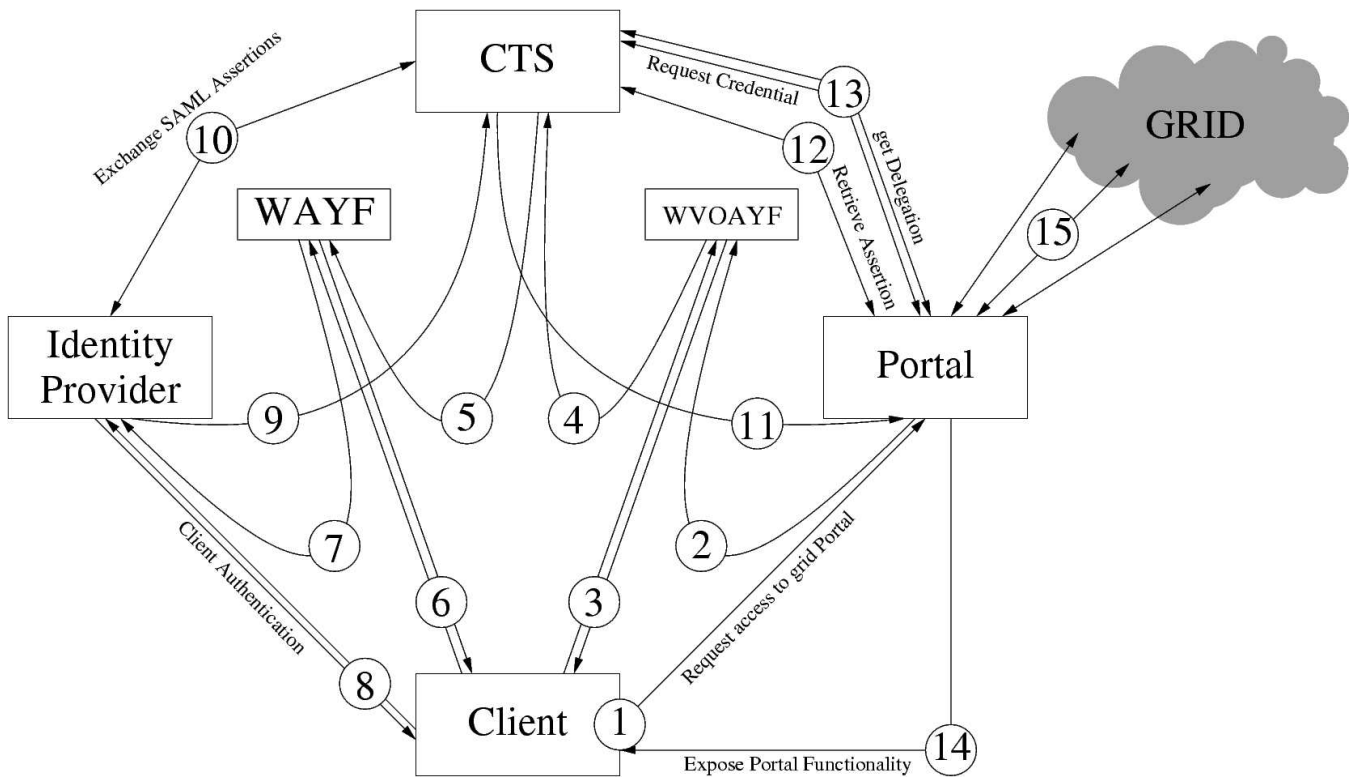
SHEBANGS and new features of MyProxy

- Use MyProxy's CA feature as CTS' back end credential manager and repository.



Complex VO structure and SHEBANGS

- Each VO server provides a CTS interface



Combining the strengths of UMIST and
The Victoria University of Manchester

GridSite and Shibboleth Integration Project

Dr. Andrew McNab & Dr. Joseph Dada

Grid Security Research Group

School of Physics & Astronomy

The University of Manchester

England

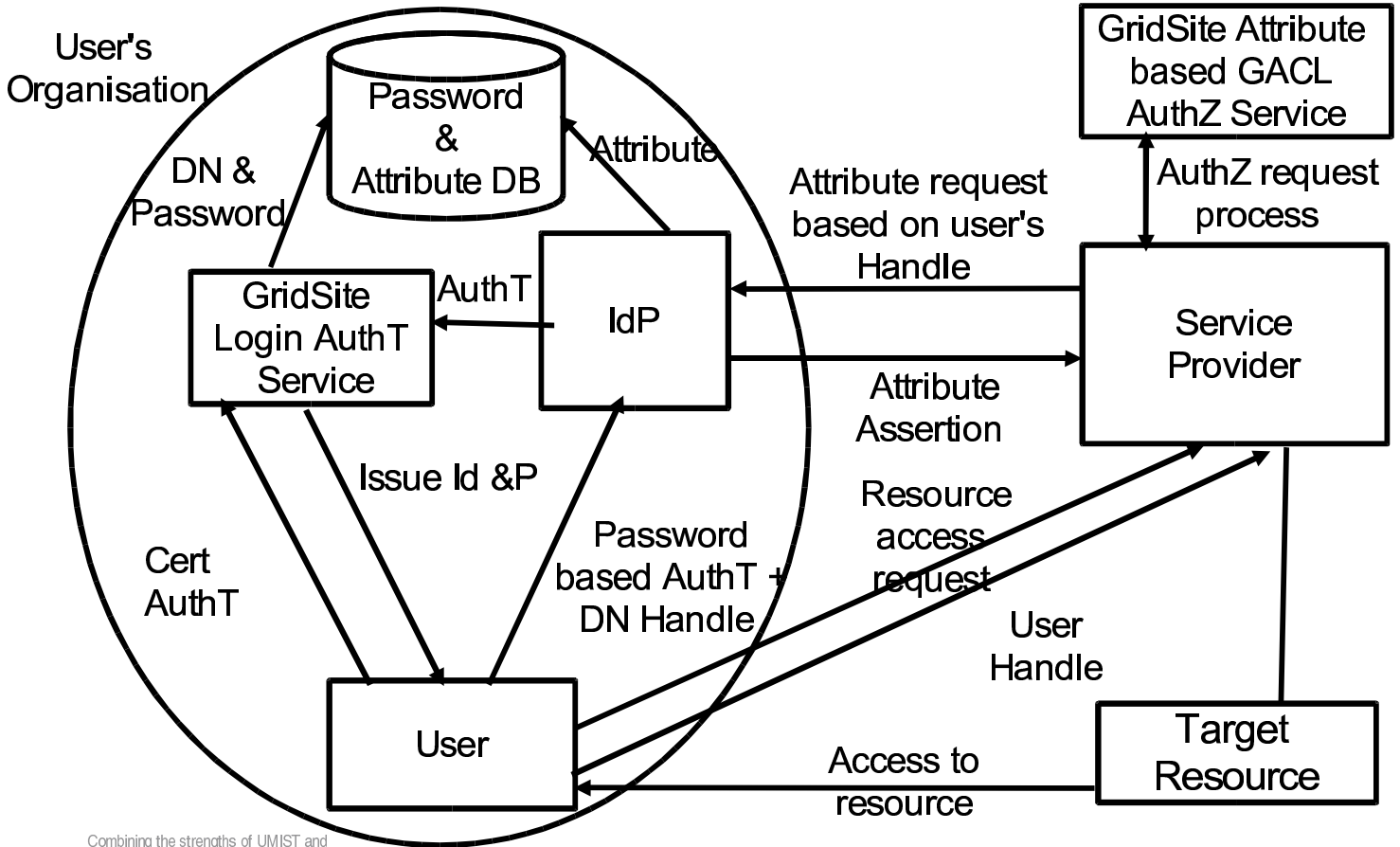
What is GridSite?

- Initially for managing and formatting the content of GridPP websites
- Based on X.509 certificate authentication method
- Authorization/access control is based on GACL
- GridSite Web Services
 - GridHTTP(S) file transfer service
 - Proxy certificate delegation service
 - Storage Resource Management web service
- Many more?

Integration Approach

- GridSite Login Authentication Service
 - Initial authentication to the Login Service using certificate
 - Issuing of temporary user name and password to the user
 - Integrate the Login Authentication Service into IdP
 - Authentication with IdP using user name & password
 - Use of DN as handle/identifier
- Integration of GridSite GACL with Service Provider
 - Apache as Policy Enforcement Point
 - GridSite as authorization engine
 - Attribute based GACL/XACML authorization
 - Apache module to integrate the attributes received by SP with GACL Authorization service

Integration Approach – Message Flow



Combining the strengths of UMIST and
The Victoria University of Manchester

Conclusion & Further Work

- A time limited password that user can use anytime anywhere to access GridSite resources
- Proxy password instead of proxy certificate
- No need to carry certificate to every computer
- Attribute-Based Access Control
- GridSite Login Authentication Service can be integrated to institution login system
- It is still a work in progress
- Further work:
 - Policy Decision Point based on XACML
 - Integration with VOMS