



GridShibPERMIS

GridShib and PERMIS Integration:

Adding Policy driven Role-Based Access Control to Attribute-Based Authorisation in Grids

The **goal** of the project is to integrate the identity federation and attribute assignment function of **Shibboleth** with the policy based enforcement function offered by the **PERMIS** access control infrastructure to authorize Grid jobs running with **Globus Toolkit** v4 in order to provide policy driven role-based access control decision making to Grid jobs.

GridShib is a research project, currently being undertaken at the University of Illinois, University of Chicago and Argonne National Laboratory, to provide Grids with the means to securely request user attributes from a Shibboleth Identity Provider (IdP). The attributes are collected by a GridShib **Policy Information Point (PIP)** and passed to a **Policy Decision Point (PDP)** which makes an access control decision based on the collected attributes and a configured access control list.

Globus Toolkit

Globus Toolkit is an open source software toolkit developed by the Globus Alliance used for building **Data Grid** systems and applications. An in-built Grid Security Infrastructure provides authorisation based on access control lists (ACLs) located at each resource

Data Grids allow large-scale distributed data processing and sharing across corporate, institutional, and geographic boundaries.

Problems with GridShib

- Users are granted access if they have any attribute in the access control list
- It is not capable of making decisions based on dynamically changing conditions such as time of day, the amount of consumed resources, etc.
- It doesn't take into account parameters of the user's request such as the operation, the requested target or the job priority, etc.
- It is not able to check if the correct set of attributes was issued by the IdP

➤ Since PERMIS is policy driven, it can test for multiple attributes and arbitrary conditions before granting access ◀

Introducing GridShibPERMIS

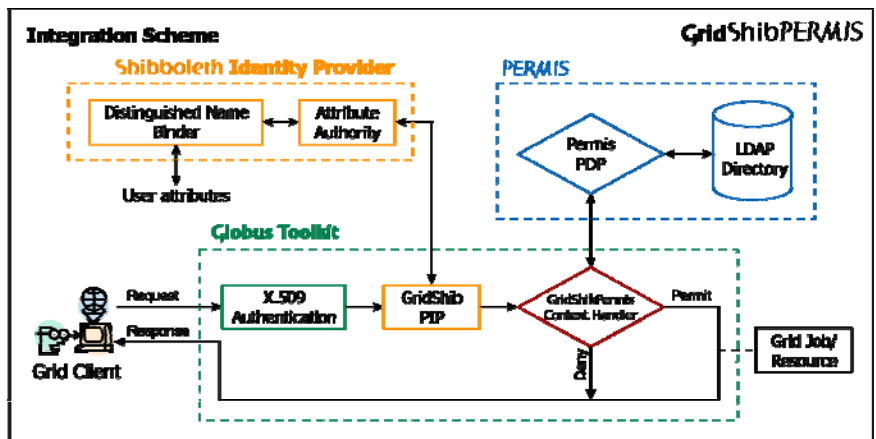
In order to carry out the integration the **GridShibPermis Context Handler** was written and the Globus authorisation chain was configured to invoke it after the GridShib PIP. The Context Handler extracts attributes returned from the Shibboleth IdP, returned as SAML attribute assertions, and converts them into the format recognized by PERMIS. It then passes them along with information about the user's requested action and resource to the PERMIS PDP via its existing Java API. The GridShibPermis Context Handler also allows X.509 attribute certificates to be returned, and these are passed to the PERMIS PDP unchanged. The PERMIS PDP first checks if the IdP is trusted to issue the attribute assertions it has returned, and then it makes an authorisation decision according to the configured PERMIS policy and the user's validated attributes.

Shibboleth

Shibboleth is an Internet2/MACE project providing cross-domain single sign-on and attribute-based authorization preserving end user privacy. The Shibboleth security protocol is based on SAML (Security Assertion Markup Language) assertions.

PERMIS

PERMIS is a policy based authorisation system (PMI - Privilege Management Infrastructure) being developed at the University of Kent, which uses X.509 attribute certificates stored in a LDAP directory to hold roles/attributes. Given a username, a resource and an action, it says whether the user is granted or denied access based on the policy for the resource.



The GridShibPermis project provides the advantages of both Shibboleth cross-organization identity federation and PERMIS policy driven role-based access controls. The project has resulted in a research paper (presented at the TERENA Networking Conference 2006) and software added to the US NMI PERMIS release.

GridShibPermis was a third-year Research Project carried out by **Andrey Novikov** [an64@kent.ac.uk] supervised by **Prof David Chadwick** [D.W.Chadwick@kent.ac.uk]

The Authors would like to thank the **UK JISC** for funding this work.

