An integrated Solution to the Security User Access in the RETELAB Grid Project, using a Web System based in Portlets and a RBAC Model by means of User Attribute Certificates and PKI.

David Mera
José M. Cotos
Pedro Saco
Andrés Gómez

IBERGRID 2008 - 2nd Iberian Grid Infrastructure Conference. Porto, 14 May, 2008

Why was RETELAB born?

- The increase of research projects and of the data they manage make the analysis of the information a tedious or impossible job.
- The community needs to access the data.
- The Oceans Study is an interdisciplinary work.
- The need of sharing resources.

What is RETELAB?

- A virtual laboratory.
- A collaborative and multidisciplinary environment.
- An environment to develop projects related to Oceanographic Remote Sensing.

RETELAB is supported upon the following ideas:

- Easy and accessible tool.
- Open Source.
- Security.
- Storage and Computational Power.

RETELAB will comprise the next modules:

- Management of the Security Access.
  - Who can have access?
  - What resources can they work with?
  - What tasks can be done over a resource?
  - Traditional Models vs RBAC.
- Storage Power.
  - Traditional ways are not enough.
  - Data GRID.

- Computational Power.
  - Just as important as the access to the data is its processing.
  - The final system must allow the execution of serial as well as parallel jobs.
  - We must include a GRID-enabled workload management which allows both modes of execution and is based on JSDL.
- Web Services.
- Deployment.
- Improvement.
- TestBeds
  - Oceanographic Applications.

RETELAB

- Universidad de Santiago de Compostela.
- Centro de Supercomputación de Galicia.
- AZTI-Tecnalia.
- Instituto Canario de Ciencias Marina.

DEVELOPMENT

We are presenting the access, management and security control of the RETELAB users.

Current Situation

- Command Line Interface.
- Computer skills are required.
- Software installation is necessary.
- Access Control Lists (by default in GT4).
- Public Key Infrastructure.

DEVELOPMENT

We propose a user system based on:

- A well balanced solution between easiness and security.
- Computer skills are not needed.
- The RBAC model.
- The Single Sign On network.

DEVELOPMENT

- Portlet based Web Portal ➔ gridsphere
- Middleware in the Grid System ➔ the globus alliance
- Register module ➔ purse-portlets
- Role management ➔ PERMIS
- Single Sign On ➔

DEVELOPMENT

- Portlets
  - Plugable Interface Components.
  - High Interoperatibility and Reuse.
- GridSphere
  - Open-source portlet based Web Portal.
  - Portlet Container.
- Globus 4
  - Middleware which provides essential Grid functionalities.

DEVELOPMENT

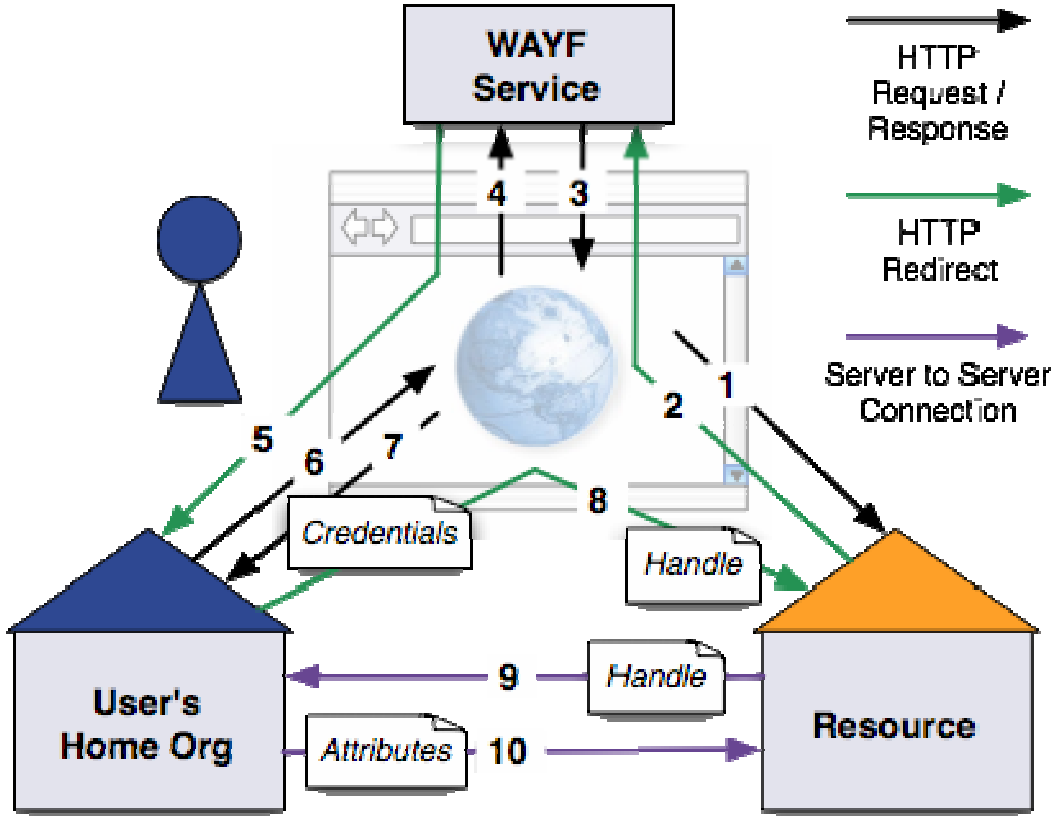
- MyProxy
  - Online credentials repository.
- PURSe
  - Earth System Grid.
  - Portlets version.
  - User register system.

DEVELOPMENT

- PERMIS
  - User access system.
  - RBAC Model.
- Shibboleth
  - Open Source.
  - Standards-based.
  - Web single sign-on across or within organizational boundaries.
  - Allows selective release of information.

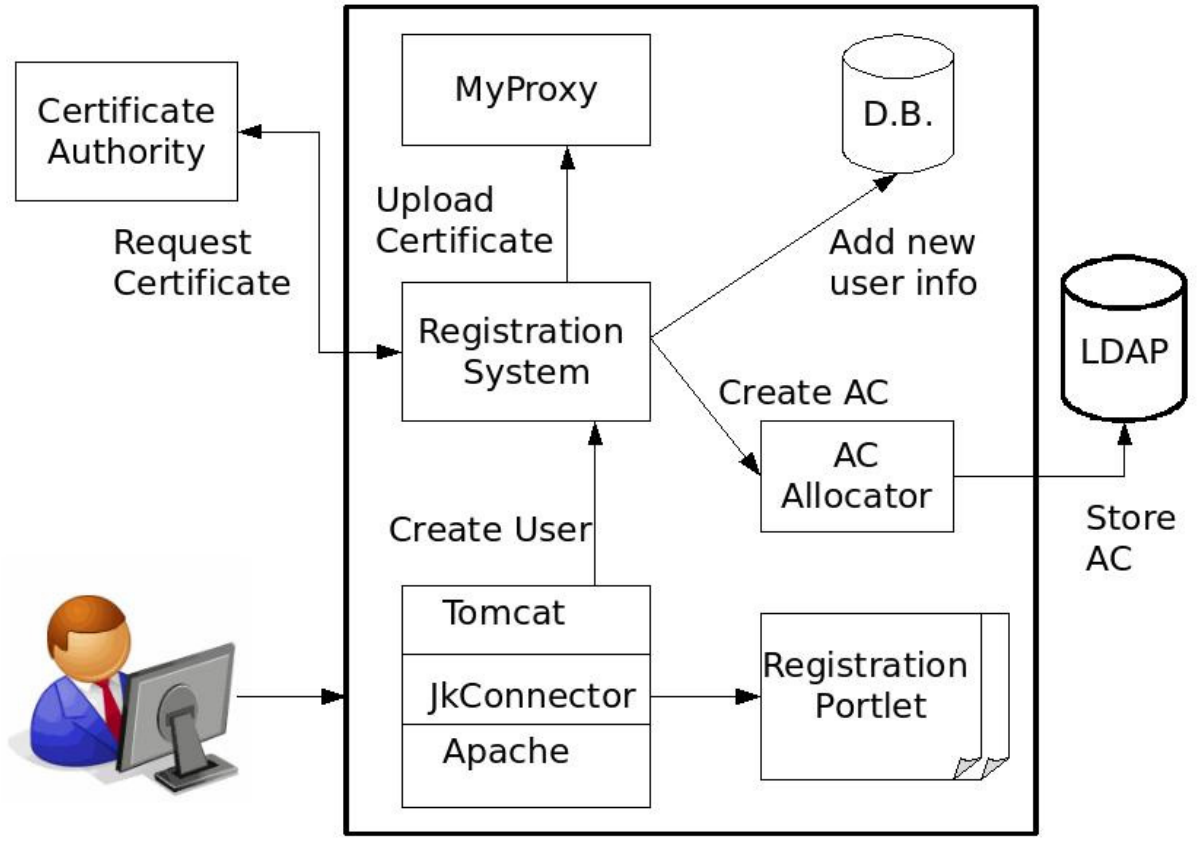
DEVELOPMENT

- Shibboleth



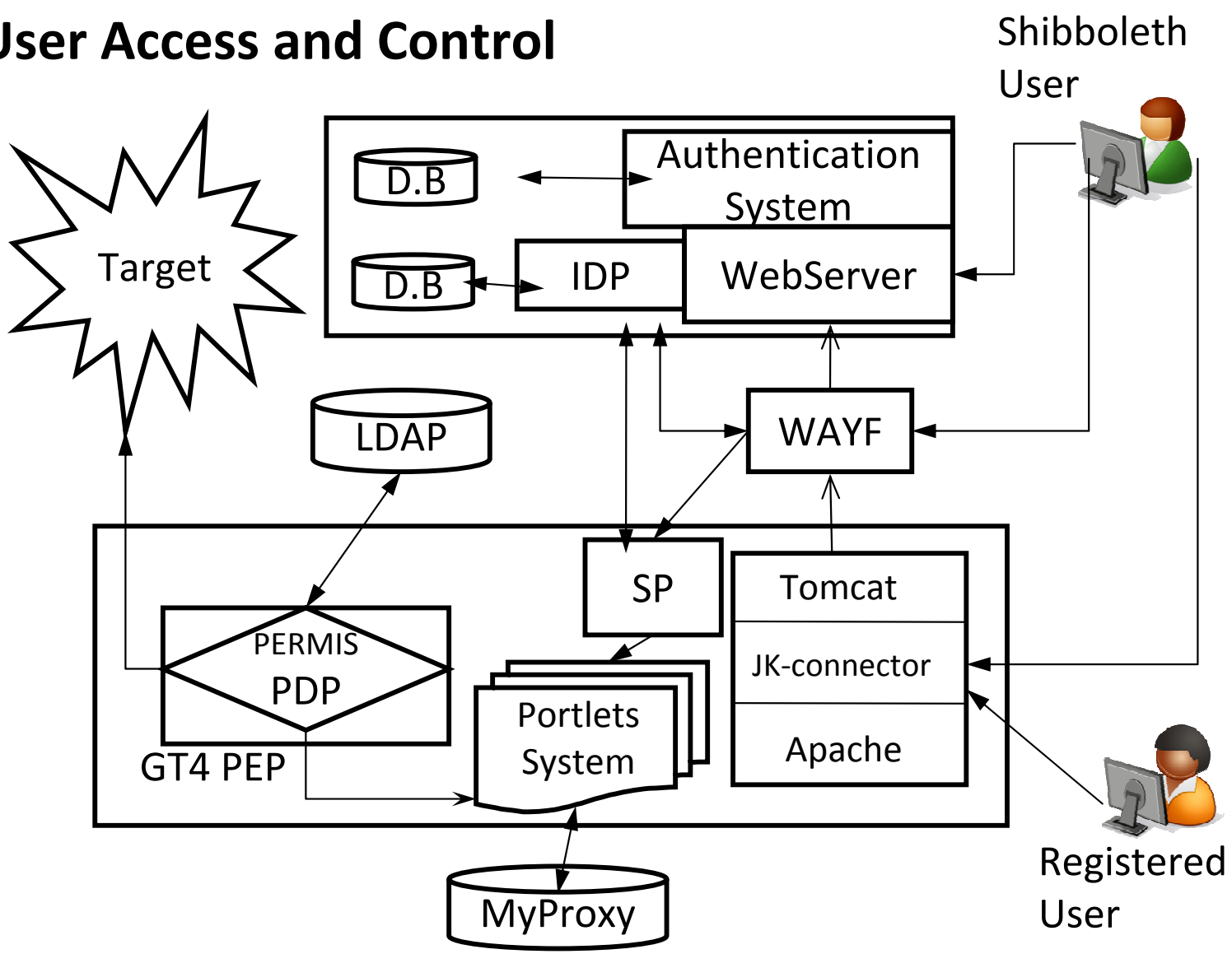
DEVELOPMENT

User Registration



DEVELOPMENT

User Access and Control

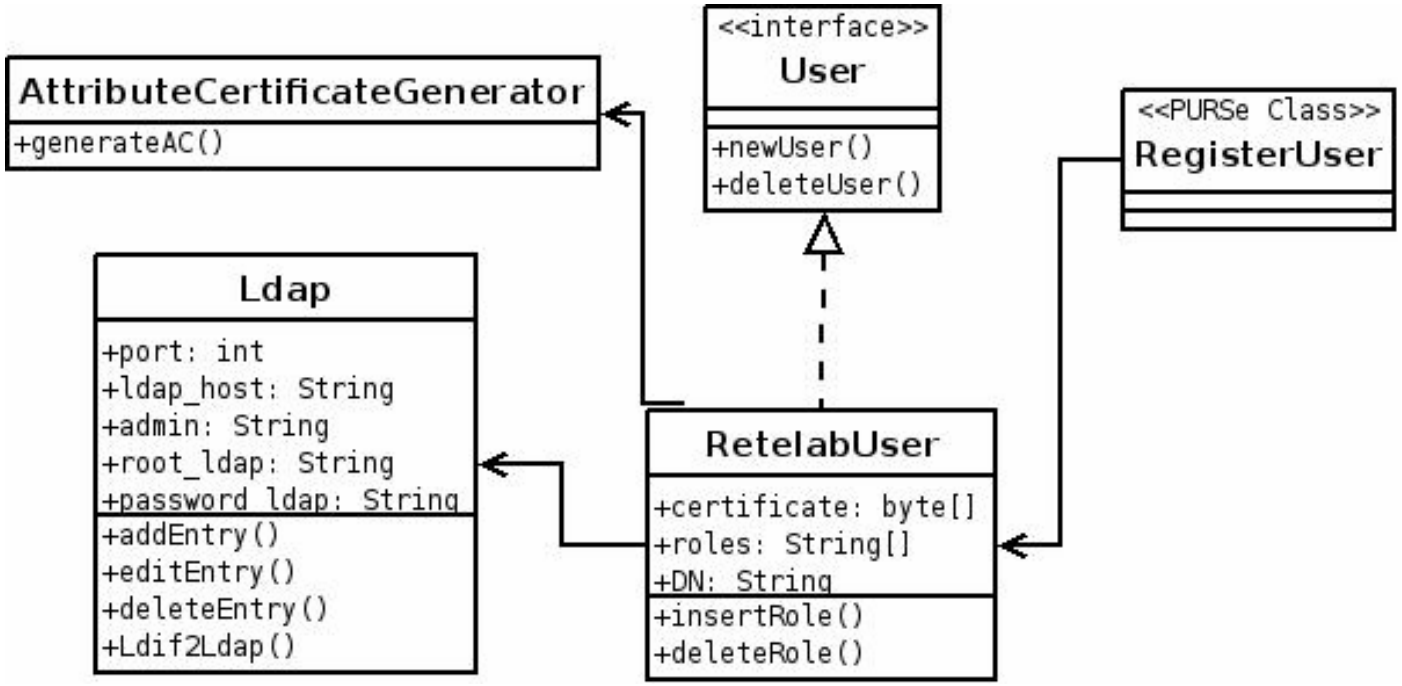


User Registration

- This module is based in PURSe Portlets.
- PURSe was modified to manage certificates in a X509 format.
- The portlets used are deployed in GridSphere.
  - PURSe was developed as a portlet for GridSphere.
  - OGCE has developed portlets for GridSphere.
  - Easy to use and to manage.

DEVELOPMENT

User Registration



Partial class diagram of a user register system

User Access and Control

- RBAC model supported by PERMIS.
- We want specific roles to be able to execute services in specific resources, but we do not want to deny the access to the rest of the services in them.
- Grid service access control.
  - PERMIS security descriptor.
  - Problems with the GRAM service control.

FUTURE

Next Works

- To finish the integration with Shibboleth.
- To deploy the system in a working environment.
- To integrate the Grid Technology with OGC Web Services standards.

An integrated Solution to the Security User Access in the RETELAB Grid Project, using a Web System based in Portlets and a RBAC Model by means of User Attribute Certificates and PKI.

David Mera
José M. Cotos
Pedro Saco
Andrés Gómez

IBERGRID 2008 - 2nd Iberian Grid Infrastructure Conference. Porto, 14 May, 2008