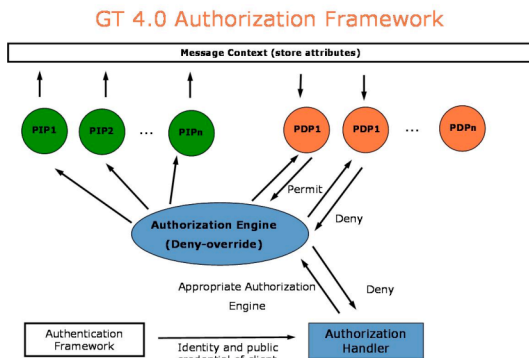




GT4 introduces a powerful and flexible authorization framework. The GT4 Java Web Services runtime invokes a series of message interceptors to process each message when it is first received (i.e., before it reaches the application). Two types of interceptors are of interest from an authorization perspective: Policy Information Points (PIPs) and Policy Decisions Points (PDPs). The figure below shows a high-level conceptual depiction of the GT4 authorization framework.



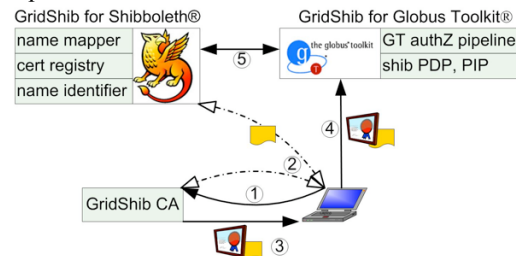
PIPs gather attribute information regarding the message. These attributes can be anything relevant to the message, but typically include information about the message subject, target resource, the requested action or the environment. This information is stored in the runtime for subsequent use by other PIPs or PDPs. PIPs act by parsing credentials presented with the request (e.g., extracting the user's distinguished name from a certificate, or extracting and parsing a VOMS attribute certificate) or by querying outside information sources (e.g., requesting attributes from a Shibboleth attribute authority). PIPs may accept information in a variety of formats, and normalize it into a technology-neutral format.

PDPs make decisions regarding whether a request should be serviced or rejected. Information collected previously by PIPs is subsequently available for use by PDPs, which return Permit or Deny decisions that are enforced by the runtime. Currently PDPs may be chained using AND logic, that is, all PDPs must return

Permit and if any returns Deny, the request is rejected. (Subsequent releases of GT 4.2 will allow for richer logic.) For example, one PDP might return Permit if a previous PIP has obtained an attribute confirming that the user is a member of an accredited virtual organization, while a second might perform a similar check for an attribute that indicates that the VO has a TeraGrid allocation.

Shibboleth and SAML Support

Shibboleth, a service developed by Internet2, implements SAML in order to allow cross-organization access to web resources. The Shibboleth-related authorization capabilities in GT4 are instantiated in several interceptors. Taken together these interceptors allow the GT4 runtime to query a Shibboleth attribute authority, obtain attributes regarding the requester, and make an access control decision based on the requester's attributes.



Functionality for Shibboleth interoperability within the GT authorization framework has been developed under the "GridShib" project [4] and include interceptors to query Shibboleth and obtain attributes, based both on the user's X.509 DN as well as identifiers passed in with the credentials, parse those attributes and then render authorization decisions as well as map the users to a local account based on those attributes.

VOMS/X.509 Attribute Certificate Support

The virtual organization membership service (VOMS), a service developed by the European DataGrid project, issues attribute assertions regarding users in the form of X.509 attribute certificates. A GT4 VOMS PIP and

PDP allow GT4 to access and process VOMS attribute certificates. The VOMS PIP parses VOMS attributes and stores them in the GT runtime. The VOMS PDP allows or denies requests based on the attributes and its configuration. The PIP and PDP can be used together to allow or deny access to a service based on the requester's VOMS attributes.

Additionally, MyProxy also now offers VOMS-based access control, allowing users to access X.509 credentials for use with the Globus Toolkit.

SAML-Based Authorization Callout

GT 4.0 implements a PDP that uses a SAML authorization query protocol, based on the specification defined by the GGF OGSA-Authorization working group [5]. This PDP calls out to external authorization services, which render and return an authorization decision that is enforced by the PDP.

Custom Authorization Modules

Besides the PIPs and PDPs described in this document, other PIPs and PDPs can be developed to interface with other authorization systems and/or to implement other authorization logic [6]. For example, GridShibPERMIS, described subsequently uses a custom PDP to take Shibboleth attributes collected by a SAML Attribute PIP and pass them to PERMIS for a decision.

Community Authorization Service as PDP

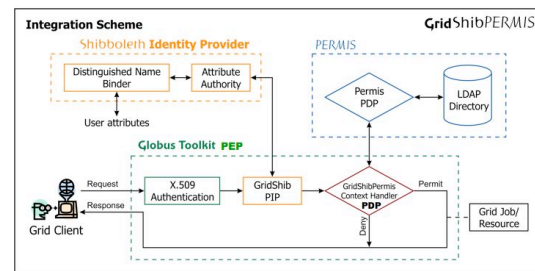
The Community Authorization Services (CAS) provides a policy service that stores user privileges. Previous version of GT allows the storage of data access privileges supported by GridFTP. A number of enhancements have been made to CAS and the GT4 web services runtime such that CAS is able to issue authorization assertions for web service invocations. Furthermore, the CAS server has been enhanced such that it can be used both in a client-pull and server-pull mode. Lastly, work is in progress that allows for co-locating a CAS service such that it can be deployed as a local PDP, and that externally defined attributes can be consumed through the PDP interface. The flexibility to choose the deployment pattern allows CAS to be tailored for individual scenarios.

XACML Support

GT 4.0 includes a prototype XACML-engine that can be configured as a PDP that can consume standardized attributes. XACML is a complex and powerful policy language with much more functionality than for example the VOMS PDP or the SAML PDP. If policy requirements go beyond the capabilities of those simple PDPs, an XACML PDP can potentially be used as an alternative.

Case Study: Integration of Globus, PERMIS and Shibboleth

An example of the pluggability of the GT Framework is demonstrated in Chadwick's work integrating Globus Security with the PERMIS authorization system and Shibboleth [2]. This integration, shown in the figure below, uses the authorization framework in GT to collect attributes from Shibboleth and passes those attributes to PERMIS through a custom PDP to render an authorization decision.



References and Contact Info

Contact: Frank Siebenlist (franks@mcs.anl.gov), Von Welch (vwelch@ncsa.uiuc.edu)

1. A Multipolicy Authorization Framework for Grid Security.
http://www-unix.globus.org/alliance/publications/papers/IEEE_NC_A_AGC.pdf
2. GridShib and PERMIS Integration: Adding Policy-driven RBAC to Attribute-based Authorisation in Grids.
http://www.terena.nl/events/tnc2006/programme/presentations/show.php?pres_id=200
3. Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, GridShib, and MyProxy.
<http://grid.ncsa.uiuc.edu/papers/gridshib-pki06-final.pdf>
4. <http://gridshib.globus.org>
5. Use of SAML for OGSF Authorization, Global Grid ForumGFD.066.
<http://www.ggf.org/documents/GFD.66.pdf>
6. <http://www-128.ibm.com/developerworks/grid/library/gr-gt4auth/>