28 April 2004
The Globus Alliance

Call for Community Testing: An OGSI Authorization Framework: Custom Authorization Plug-ins and Authorization Callout in GT 3.3.0

What is a "Call for Community Testing"?

A Call for Community Testing is a mechanism to notify our users that new Globus code is available for testing in the field. Through these calls, the Globus Alliance hopes to expose its code to a wide variety of usage scenarios early in its development process. The ultimate goals are to catch bugs that have historically been found only after final releases, and to elicit feedback from the community on ways our software can be improved.

Participating in a Testing Call is Easy!

1. *Optional:* Consider sending mail to testing@globus.org to let us know that you're helping out and describing what you intend to test
2. Install the software in a non-production environment: Use the 3.3.0 distribution from http://www-unix.globus.org/toolkit/downloads/development/
3. Exercise the code as described in the documentation.
4. Log your experiences in http://bugzilla.globus.org/globus/ under GT3/Security, version "development". Please mention 3.3.0 explicitly in the body of the report.
5. *Optional:* Consider sending descriptions of your tests to testing@globus.org so that we might use them to build standard tests in the future

If you have any questions or comments about the process, feel free to contact Bob Gaffaney at gaffaney@mcs.anl.gov.

Continued on next page

The Testing Period For This Call: 28 April – 30 June 2004

About Authorization

The current production release of the Globus Toolkit, GT 3.2, includes simple authorization mechanisms based on identity. With this release, we have added support for extending GT's authorization capabilities in two ways:

- Through pluggable custom authorization modules; and
- Using a SAML-based authorization callout to consult with a authorization service..

Plugging in a custom authorization module allows the replacement of the normal GT authorization mechanisms with an arbitrary method. This method can be any Java class that conforms to the GT authorization framework and could be used, for example, to integrate GT with an existing site mechanism, have GT use a third-party authorization library, or implement a new authorization scheme.

This callout directs all authorization requests to an OGSA-Authorization compliant authorization service using the SAML protocol for sending queries and receiving decisions. The authorization service can use existing authorization libraries, for example, the PERMIS developers have created such a service. The callout allows a number of GT installations to share a single authorization service and allows for centralized policy management.

Reasons for testing Authorization

These advanced authorization features are aimed at the following users:

1. Users who have existing site authorization systems they want to integrate into GT.

2. Developers of advanced authorization systems who want to integrate support for their system into GT.

3. Researchers who wish to experiment with different authorization schemes in the context of Grids.

Our goal is to allow these users to easily integrate their work with the GT authorization framework and we are seeking feedback from these users as to how well these new features meet their needs.

Continued on next page

Components affected by Authorization

The new authorization callouts and plug-ins will work with any of the OGSI-based portions of GT3, including GRAM and any custom service built on the OGSI framework.

Environment/build parameters and other special conditions to test

We are interested in having users use both custom authorization plug-ins and the authorization callout. We would particularly be interested in those who can test the following:

1. Exception cases: authorization plug-ins and services that fail in unusual ways. GT should handle these failures gracefully.
2. Poorly formed responses. Again, GT should handle these with a graceful authorization failure.

Documentation/For more information

Refer to section 4.3.3 (Service Authorization settings) in ogsa/docs/message_security.html for information on configuring a custom authorization mechanism, and for using SAML Authorization callout to dispatch authorization queries to an authorization service.

For documentation about writing OGSA-Authorization compliant authorization service, please refer to ogsa/docs/authz_service_impl.html.

The Testing Period For This Call: 28 April – 30 June 2004