GSI Admission Control and Identity Mapping Callout Specification

Draft 1/28/2003

This is a proposed specification for addition of callouts for Admission Control and Identity Mapping to be added to the Globus Toolkit (GT2). If implemented it would appear in a post GT2.2 release probably in early 2003.

NOTE: This is a proposed modification. It is still a draft and no commitment has been made as to implementation yet.

Comments and questions to Von Welch (welch@mcs.anl.gov)

1 Overview

This specification defines modifications to the Globus Toolkit version 2.x (GT2) to enable two new features:

1. Enable a site to override the grid-mapfile as the means of mapping the grid credentials to local identity.
2. Enable a site to install site-specific admission control checks based on the credentials of incoming clients.

These changes are driven by sites that have, or wish to have, centralized infrastructure for admission control (determining who is allowed to connect to a service) and identity mapping. These changes will allow these sites to plug in their own modules for interfacing with their infrastructure.

2 Goals

Goals behind these changes:

- Allows sites to develop and plug in modules to do admission control and identity mapping into GT2 GRAM and GridFTP services (TBD: Will MDS use these modifications?)
- Ease of use. Development and installation of modules should be as easy as possible.
- Flexibility: Arbitrary methods of admission control and identity mapping should be allowed.
- Able to support complex policies: If desired, a site could write a single module that wrapped a number of actual checks with custom logic to implement complex policies.
- Minimal modifications. Ideally all changes will be contained in the GSI libraries and require as few modifications to calling applications (e.g. Gatekeeper) as possible.

- Ease of implementation. This is meant to be a modification to fix some immediate requirements, not a long-term authorization solution. Hence we want to keep development time to a minimum.
- Sites that do not wish to use these modifications should not be aware of them. They should have no impact on usage and impact reliability as little as possible.
- Work with a GT2 installation using Kerberos instead of GSI.
- Work with credential contents. Sites have expressed the desire to do more than identity-based admission control and mapping, so we want to provide means to access more than just the identity of the client.
- Protection of calling application. The calling application should be protected as much as possible from misbehavior of plugins.

3 Non-Goals

A specific non-goal behind these changes is supporting fine-grain authorization based on application-specific attributes of the user's request (e.g.RSL, MDS query, GridFTP operation). One or more authorization API will need to be developed for this and the changes proposed in this document do not attempt to solve this problem.

The Globus Project itself plans on providing no modules for use with these modifications (beyond maybe a simple example). It is expected that sites will develop and share implementations to meet their needs.

4 Overriding the Grid-mapfile

GT2 will provide the following interface (exact method TBD) to a function for doing identity mapping from Grid credentials to a local identity. Sites will be able to replace the normal function that uses the grid-mapfile with one they develop.

Parameters:

- *gss_context*: The GSS context as created by the calling service with the client through the gss_init/accept_sec_context() proceedure. (Input, const)
- *service_name*: A NUL-terminated string indicating the name of the service being requested by the client. Initially this will be either "gridftp" or the name of the service passed to the gatekeeper (e.g. "jobmanager-lsf"). May be NULL if this information is unavailable to the caller. (Optional, Input, const)
- *identity_string*: A buffer to be filled in by the caller on success indicated the local identity the user should be mapped to (as a NUL-terminated string). Length of this string is given by *indentity_string_len*. (Note that the function should verify this buffer is long enough and return error if it is not) (Output)
- *identity_string_len*: The length of the *identity_string* buffer. (Input, const)

Return code:

- *globus_result_t*: Inidicating success or failure (in which case it's a globus error object).

5 Enabling Admission Control Checks

GT2 will provide the following interface to zero or more function calls for doing addmission control checks based on Grid credentials. Sites will be able to install functions they develop. Exact method of installing these checks TBD.

Parameters:

- *gss_context*: The GSS context as created by the calling service with the client through the gss_init/accept_sec_context() proceedure. (Input, const)
- *service_name*: A NUL-terminated string indicating the name of the service being requested by the client. Initially this will be either "gridftp" or the name of the service passed to the gatekeeper (e.g. "jobmanager-lsf"). May be NULL if this information is unavailable to the caller. (Optional, Input, const)

Return code:

- *globus_result_t*: Indicating success (Admission succeeded. Calling application should proceed with other checks and mapping) or failure (Admission control failed and calling application should not proceed).

6 Related functionality

1. Plug-in needs to be able to pull identity from gss_context, this is available today with standard GSSAPI calls.
2. Plug-in needs to be able to pull certificate chain from gss_context. This functionality should be implemented by gss_inquire_context_by_oid().