GT 5.0.0 GSI C: Developer's Guide

Introduction

This component provides an API for authentication and two APIs for authorization.

The authentication API is an implementation of the GSS-API (RFC 2743 and RFC 2744) extended with the functions described in the GSS-API Extensions document.

On the authorization front there is a coarse-grained API, which in addition to authorizing also provides a mapping function, and an API that allows finer grained authorization decisions to be made. The finer grained API follows the subject, object, action paradigm.

Both of the authorization APIs allow different back end implementations through the use of dynamic library loading.
# Table of Contents

1. Before you begin .............................................................................................................. 1  
   1. Feature summary .............................................................................................................. 1  
   2. Tested platforms .............................................................................................................. 1  
   3. Backward compatibility summary ..................................................................................... 1  
   4. Technology dependencies ................................................................................................ 1  
   5. Security considerations for GSI C ..................................................................................... 2  
2. Usage scenarios .................................................................................................................. 3  
3. Tutorials ............................................................................................................................... 4  
4. Architecture and design overview ....................................................................................... 5  
   1. Authentication .................................................................................................................. 5  
   2. Authorization ................................................................................................................... 6  
5. APIs ..................................................................................................................................... 7  
6. Protocol Specifications ........................................................................................................ 9  
   1. GSI Message Specification .............................................................................................. 9  
1. GSI Commands ................................................................................................................... 10  
   grid-cert-diagnostics ........................................................................................................... 11  
   grid-cert-info ..................................................................................................................... 13  
   grid-cert-request ............................................................................................................... 15  
   grid-default-ca .................................................................................................................... 19  
   grid-change-pass-phrase ................................................................................................. 21  
   grid-proxy-init .................................................................................................................... 22  
   grid-proxy-destroy ............................................................................................................. 25  
   grid-proxy-info ................................................................................................................... 26  
   grid-mapfile-add-entry ........................................................................................................ 28  
   grid-mapfile-check-consistency .......................................................................................... 29  
   grid-mapfile-delete-entry .................................................................................................... 30  
7. Configuring Certificates ................................................................................................. 31  
   1. Configuring Globus to Trust a Particular Certificate Authority ..................................... 31  
   2. Configuring Globus to Create Appropriate Certificate Requests .................................... 32  
   3. Requesting Service Certificates ..................................................................................... 34  
   4. Configuring Credential Mappings ................................................................................... 34  
   5. GSI File Permissions Requirements ............................................................................... 36  
8. Environment variable interface .......................................................................................... 38  
   1. Environmental Variables for GSI C .................................................................................. 38  
9. Debugging ........................................................................................................................ 42  
10. Troubleshooting .............................................................................................................. 43  
   1. Credential Troubleshooting ............................................................................................. 43  
   2. Grid map Troubleshooting ............................................................................................... 46  
11. Related Documentation ................................................................................................. 47  
Glossary ................................................................................................................................. 48
List of Tables

1. Command line options ..................................................................................................................... 21
2. Command line options ..................................................................................................................... 23
3. Command line options ..................................................................................................................... 25
4. Command line options ..................................................................................................................... 26
5. Print options .................................................................................................................................. 26
6. Validity options .............................................................................................................................. 27
7. Command line options ..................................................................................................................... 28
8. Command line options ..................................................................................................................... 29
9. Command line options ..................................................................................................................... 30
  7.1. CA files ..................................................................................................................................... 31
10. Command line options ..................................................................................................................... 32
  7.2. Certificate request configuration files .......................................................................................... 32
  7.3. Certificate request files ............................................................................................................... 34
  7.4. Gridmap File Location Algorithm ............................................................................................... 35
  7.5. Authorization Configuration File Locations ................................................................................ 36
  7.6. Authorization Configuration File Locations ................................................................................ 36
10.1. Credential Errors ........................................................................................................................ 44
10.2. Gridmap Errors .......................................................................................................................... 46
Chapter 1. Before you begin

1. Feature summary

Features new in GT 5.0.0

- Support for processing host certificates containing X.509 subjectAltName extensions with dNSName or iPAddress values.

Other Supported Features

- Authentication of user using standard X.509 End Entity and Proxy Certificates.
- Delegation using X.509 Proxy Certificates.
- Pluggable authorization based on the client's certificate chain for GridFTP and GRAM2.
- Pluggable authorization for GRAM2 based on the RSL of the job.

Deprecated Features

- None

2. Tested platforms

Tested platforms for GSI C:

- i386 Linux

3. Backward compatibility summary

Protocol changes in GSI C since GT 4.2.x

- None

API changes since GT 4.2.x

- None

Exception changes since GT 4.2.x

- Not applicable

Schema changes since GT 4.2.x

- Not applicable

4. Technology dependencies

The GSI C component depends on the following GT components:

- C Common Libraries
The GSI C component depends on the following 3rd party software:

- OpenSSL

## 5. Security considerations for GSI C

- During host authorization, the toolkit treats host names of the form "hostname-ANYTHING.edu" as equivalent to "hostname.edu". This means that if a service was set up to do host authorization and hence accept the certificate "hostname.edu", it would also accept certificates with DNs "hostname-ANYTHING.edu".

The feature is in place to allow a multi-homed host following a "hostname-interface" naming convention, to have a single host certificate. For example, host "grid.test.edu" would also accept the likes of "grid-1.test.edu" or "grid-foo.test.edu".

🎉 **Note**

The string ANYTHING matches only the name of the host and not domain components. This means that "hostname.edu" will not match "hostname-foo.sub.edu", but will match "host-foo.edu".

🎉 **Note**

If a host was set up to accept "hostname-1.edu", it will not accept "hostname-ANYTHING.edu" but will accept "hostname.edu". That is, only one of the names being compared may contain the hyphen character in the host name.

A bug\(^1\) has been opened to see if this feature needs to be modified.

In GT 5.0.0, it is possible to disable this behavior, by setting the environment variable GLOBUS_GSS-API_NAME_COMPATIBILITY to STRICTRFC2818.

---

\(^1\) [http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2969](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2969)
Chapter 2. Usage scenarios

There is no content available at this time.
Chapter 3. Tutorials

There are no tutorials available at this time
Chapter 4. Architecture and design overview

1. Authentication

As mentioned in the introduction, the GSI C security framework uses the GSSAPI API and extensions to it to abstract security mechanism specific details. Below the GSSAPI layer there exist multiple APIs for dealing with credential management, X.509 certificates in general and proxy certificates in particular as well as security configuration. Each of these APIs is described in more detail below.

The general design principle guiding these APIs is data encapsulation. Data structures (handles and attributes) capture and encapsulate the state of the system. These data structures are then acted upon by various getters and setters, as well as other functions.

1.1. The GSS Assist API

The GSS Assist API provides helper functions wrapping the process of security (GSS) context establishment, support for gridmap authorization and various other helper functions that wrap GSSAPI functions and capture common usage.

1.2. GSSAPI

The GSSAPI implementation provided by the toolkit is based upon SSL/TLS with extensions to the standard path validation mechanism to handle proxy certificates. It relies upon the credential and certificate utility APIs for general certificate acquisition and inspection functionality.

1.3. The Callback API

This API provides a callback that can be plugged into the OpenSSL path validation framework. This callback provides the additions to path validation required for dealing with proxy certificates and X.509 extensions. Furthermore, it allows applications to inspect data, e.g. the validated certificate chain, after the validation is done.

1.4. The Certificate Utilities API

The Certificate Utilities API provides helper functions for dealing with X.509 certificates. This API does not use the "handle" concept mentioned in the introduction. Rather, it operates on datatypes provided by the OpenSSL APIs.

1.5. The Credential API

The Credential API deals with reading and writing certificates from and to the file system and the OpenSSL I/O abstraction layer. It also provides functions for inspecting and validating the read credentials.

1.6. The Proxy APIs

The Proxy APIs provide a implementation of the X.509 Proxy Certificate Extension ASN.1 structure as well as functions for creating new proxies.
1.7. The System Configuration API

This API serves as an abstraction layer for OS specific information needed by the security infrastructure. It provides OS specific functions for discovering certificates from a set of predefined standard locations as well as functions for doing the same for various configuration files.

2. Authorization

As described in the introduction the GSI C security framework essentially provides two authorization APIs, the generic Authorization API and the Gridmap API. These APIs differ in various ways:

The Authorization API provides a framework that allows callouts to 3rd party authorization solutions, does not provide a default authorization mechanism and is geared to authorizing the subject-action-object tuple.

The Gridmap API on the other hand, while allowing for custom callouts to be plugged in and override the default behavior, provides a default authorization and mapping mechanism based on the grid map file. Also, it only furnishes the callouts with information about the entity to be authorized, i.e. it does not provide information on the action and the object, so it is somewhat simpler in its approach. Finally, it provides the ability to map authorized entities to local system entities, e.g. UNIX user names. More information on the interface used for Gridmap callouts can be found here.

1 ../GSIAuthorizationCalloutSpecification-04.pdf
Chapter 5. APIs

Documentation for the APIs in this component can be found here:

- `gaa_core` [no frames]
- `gaa_gss_generic` [no frames]
- `gaa_plugin` [no frames]
- `globus_auth` [no frames]
- `globus_authz_callout_error` [no frames]
- `globus_gridmap_callout_error` [no frames]
- `globus_gsi_callback` [no frames]
- `globus_gsi_cert_utils` [no frames]
- `globus_gsi_credential` [no frames]
- `globus_gsi_openssl_error` [no frames]
- `globus_gsi_proxy_core` [no frames]
- `globus_gsi_proxy_ssl` [no frames]
- `globus_gsi_sysconfig` [no frames]
- `globus_gss_assist` [no frames]

• globus_gssapi_gsi\textsuperscript{29} [no frames\textsuperscript{30}]
• globus_openssl_module\textsuperscript{31} [no frames\textsuperscript{32}]
• gssapi_error\textsuperscript{33} [no frames\textsuperscript{34}]

For information on the internationalization API, see the CCommon Libraries Public Interface.

\textsuperscript{29} http://www.globus.org/api/c-globus-4.0/globus_gssapi_gsi/html/index.html#_top
\textsuperscript{30} http://www.globus.org/api/c-globus-4.0/globus_gssapi_gsi/html/main.html
\textsuperscript{31} http://www.globus.org/api/c-globus-4.0/globus_openssl_module/html/index.html#_top
\textsuperscript{32} http://www.globus.org/api/c-globus-4.0/globus_openssl_module/html/main.html
\textsuperscript{33} http://www.globus.org/api/c-globus-4.0/gssapi_error/html/index.html#_top
\textsuperscript{34} http://www.globus.org/api/c-globus-4.0/gssapi_error/html/main.html
Chapter 6. Protocol Specifications

1. GSI Message Specification

The GSSAPI implementation contained in this component produces security tokens that follow an extended version of the SSL/TLS protocol. More information about the protocol can be found here¹.

¹ ../GSI-message-specification-02.doc
GSI Commands
**Name**

grid-cert-diagnostics -- Print diagnostic information about certificates and keys

grid-cert-diagnostics [-h] [-p]

**Description**

The **grid-cert-diagnostics** command displays information about the current user's security environment, including information about security-related environment variables, security directory search path, personal key and certificates, and trusted certificates. It is intended to provide information to help diagnose problems using GSI security.

The full set of command-line options to **grid-cert-diagnostics** consists of:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>Display a help message and exit</td>
</tr>
<tr>
<td>-p</td>
<td>Display information about the personal certificate and key that is the current user's default credential.</td>
</tr>
</tbody>
</table>

**Examples**

In this example, we see the default mode of checking the default security environment for the system, without processing the user's key and certificate. Note the user receives a warning about a `cog.properties` and about an expired CA certificate.

```
% grid-cert-diagnostics

Checking Environment Variables
================================
Checking if X509_CERT_DIR is set... no
Checking if X509_USER_CERT is set... no
Checking if X509_USER_KEY is set... no
Checking if X509_USER_PROXY is set... no

Checking Security Directories
================================
Determining trusted cert path... /etc/grid-security/certificates
Checking for cog.properties... found
WARNING: If the cog.properties file contains security properties, Java apps will ignore the security paths described in the GSI documentation

Checking trusted certificates...
================================
Getting trusted certificate list...
Checking CA file /etc/grid-security/certificates/1c4f4c48.0... ok
Verifying certificate chain for "/etc/grid-security/certificates/1c3f2ca8.0"... ok
Checking CA file /etc/grid-security/certificates/9d8788eb.0... ok
Verifying certificate chain for "/etc/grid-security/certificates/9d8753eb.0"... failed
  globus_credential: Error verifying credential: Failed to verify credential
  globus_gsi_callback_module: Could not verify credential
  globus_gsi_callback_module: The certificate has expired:
```

---

11
Credential with subject: /DC=org/DC=example/OU=grid/CN=CA has expired.

In this example, we show a user with a mismatched private key and certificate:

% grid-cert-diagnostics -p

Checking Environment Variables
================================
Checking if X509_CERT_DIR is set... no
Checking if X509_USER_CERT is set... no
Checking if X509_USER_KEY is set... no
Checking if X509_USER_PROXY is set... no

Checking Security Directories
=============================
Determining trusted cert path... /etc/grid-security/certificates
Checking for cog.properties... not found

Checking Default Credentials
================================
Determining certificate and key file names... ok
Certificate Path: "/home/juser/.globus/usercert.pem"
Key Path: "/home/juser/.globus/userkey.pem"
Checking certificate... ok
Checking private key... ok
Checking Certificate Subject...
"/O=Grid/OU=Example/OU=User/CN=Joe User"
Checking cert... ok
Checking key... ok
Checking that certificate contains an RSA key... ok
Checking that private key is an RSA key... ok
Checking that public and private keys have the same modulus... failed

Certificate and and private key don't match
Name

grid-cert-info -- Display certificate information

grid-cert-info [-help] [-version] 
[-file CERTIFICATE-FI- 

Description

The grid-cert-info displays information from a user's credential, or from any X.509 certificate if the -file CERTI- 
IFICATE-FI- 
LENAME is used. By default, a text representation of the entire certificate is displayed. If more than one 
display option is present on the command line, the output is generated in the order the options occur on the command 
line.

The following search order is used to locate the default certificate:

- $X509_USER_CERT
- $HOME/.globus/usercert.pem
- $HOME/.globus/usercred.p12

If the certificate is encoded in pkcs12, grid-cert-info will prompt for the password used to protect the .p12 file.

The full set of command-line options to grid-cert-info is:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help</td>
<td>Print help information and exit</td>
</tr>
<tr>
<td>-version</td>
<td>Print version information and exit</td>
</tr>
<tr>
<td>-file</td>
<td>Read credential from CERTIFICATE-FI-LENAME instead of the default location.</td>
</tr>
<tr>
<td>-subject</td>
<td>Print the subject name of the certificate.</td>
</tr>
<tr>
<td>-issuer</td>
<td>Print the subject name of the issuer of the certificate.</td>
</tr>
<tr>
<td>-issuerhash</td>
<td>Print the hash of the name of the issuer of the certificate.</td>
</tr>
<tr>
<td>-startdate</td>
<td>Print the date and time from which the certificate is valid</td>
</tr>
<tr>
<td>-enddate</td>
<td>Print the date and time when the certificate expires.</td>
</tr>
</tbody>
</table>

Examples

Print out the date range when a certificate is valid:

% grid-cert-info -startdate -enddate

Oct 29 13:09:42 2007 GMT
Oct 28 13:09:42 2008 GMT
Note that in this example, the start date is printed first, based on the order of the command-line options.

**Limitations**

The `-issuerhash` fails with some versions of OpenSSL.
Name

grid-cert-request -- Create a certificate request

[-commonname NAME] [-service SERVICE] [-host FQDN] [-dns FQDN,...] [-ip IP-ADDRESS,...] [-interactive]
[-dir DIRECTORY] [-prefix PREFIX] [-ca [HASH]] [-nopw]

Description

grid-cert-request generates a public/private key pair an X.509 certificate request containing the public key and a subject name. By default, it generates a request for a user certificate for the invoking user. grid-cert-request can also be used to create host or service certificates based on command-line options. At least one Certificate Authority must be configured to use with the Globus Toolkit in order for this command to succeed.

Complete set of options to grid-cert-request is:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help</td>
<td>Print help information and exit</td>
</tr>
<tr>
<td>-version</td>
<td>Print version information and exit</td>
</tr>
<tr>
<td>-verbose</td>
<td>Don’t clear screen after running OpenSSL</td>
</tr>
<tr>
<td>-force</td>
<td>Overwrite an existing certificate request if present.</td>
</tr>
<tr>
<td>-commonname NAME</td>
<td>Construct a subject name with NAME as the final name component. By default, the subject name is inferred from the output of the finger program. If that fails, grid-cert-request will prompt of a name.</td>
</tr>
<tr>
<td>-service SERVICE</td>
<td>Construct a subject name with the common name constructed from the SERVICE name and the hostname joined by the / character. The -service requires that the -host option also be used. The private key created for a service certificate request is not encrypted.</td>
</tr>
<tr>
<td>-host FQDN</td>
<td>Construct a subject name with FQDN as the name of the host. This must be a fully-qualified name in dotted string notation (e.g. grid.example.org). If no service is specified by the -service option, the subject name will be host/FQDN. The private key created for a host certificate request is not encrypted. By default the host certificate request and key are created in /etc/grid-security.</td>
</tr>
<tr>
<td>-dns FQDN,...</td>
<td>Add a subjectAltName extension to the certificate request containing one or more DNS names separated by the comma (, ) character. These names may contain the wildcard character (*). Globus Toolkit 4.2.1 and later will process the subjectAltName extension if present when performing mutual authentication with a service.</td>
</tr>
<tr>
<td>-ip IP-ADDRESS,...</td>
<td>Add a subjectAltName extension to the certificate request containing one or more IP address values separated by the comma (, ) character. Globus Toolkit 4.2.1 and later will process the subjectAltName extension if present when performing mutual authentication with a service when the client is presented with an IP address as input.</td>
</tr>
<tr>
<td>-interactive</td>
<td>Interactively prompt for the components of the certificate subject name.</td>
</tr>
<tr>
<td>-dir DIRECTORY</td>
<td>Write the certificate request and key to DIRECTORY, creating it if the directory does not exist. By default, the certificate request and key are placed in $HOME/.globus.</td>
</tr>
<tr>
<td>-prefix PREFIX</td>
<td>Prepend the string PREFIX to the certificate, key, and request filenames. The default prefix is user for user certificates and host for host certificates.</td>
</tr>
</tbody>
</table>
| -ca HASH | Choose a non-default Certificate Authority configuration to construct the certificate request. If HASH is present on the command line, then grid-cert-request will use
that certificate authority's configuration. Otherwise, it will prompt the user for a CA to choose from the list of configured CAs.

Create a private key without a password. This may be a security risk if the file permissions of the private key are not carefully maintained.

### Examples

Request a user certificate:

```
% grid-cert-request
```

A certificate request and private key is being created.
You will be asked to enter a PEM pass phrase.
This pass phrase is akin to your account password,
and is used to protect your key file.
If you forget your pass phrase, you will need to obtain a new certificate.

Generating a 1024 bit RSA private key
.....................++++++
........++++++
writing new private key to '/home/juser/.globus/userkey.pem'
Enter PEM pass phrase:

A private key and a certificate request has been generated with the subject:

/O=Grid/OU=Example/OU=User/CN=Joe User

If the CN=Joe User is not appropriate, rerun this script with the -force -cn "Common Name" options.

Your private key is stored in /home/juser/.globus/userkey.pem
Your request is stored in /home/juser/.globus/usercert_request.pem

Please e-mail the request to the Globus Certificate Service ca@grid.example.org
You may use a command similar to the following:

```
cat /home/juser/.globus/usercert_request.pem | mail ca@grid.example.org
```

Only use the above if this machine can send AND receive e-mail. If not, please mail using some other method.

Your certificate will be mailed to you within two working days.
If you receive no response, contact Globus Certificate Service at ca@grid.example.org

Request a host certificate, putting the request and key files in the $HOME/.globus/host directory.

```
% grid-cert-request -host grid.example.org -dir $HOME/.globus/host
```
A private host key and a certificate request has been generated with the subject:

/O=Grid/OU=Example/OU=User/CN=host/grid.example.org

The private key is stored in /tmp/examplegrid/hostkey.pem
The request is stored in /tmp/examplegrid/hostcert_request.pem

Please e-mail the request to the Globus Certificate Service ca@grid.example.org
You may use a command similar to the following:

    cat /tmp/examplegrid/hostcert_request.pem | mail ca@grid.example.org

Only use the above if this machine can send AND receive e-mail. If not, please mail using some other method.

Your certificate will be mailed to you within two working days.
If you receive no response, contact Globus Certificate Service at ca@grid.example.org

Request a host certificate with subjectAltName extensions. This certificate is valid for hosts with DNS names execution.example.org and transfer.example.org.

% grid-cert-request -host grid.example.org -dns execution.example.org,transfer.example.org

A private host key and a certificate request has been generated with the subject:

/O=Grid/OU=Example/OU=User/CN=host/grid.example.org

The private key is stored in /tmp/examplegrid/hostkey.pem
The request is stored in /tmp/examplegrid/hostcert_request.pem

Please e-mail the request to the Globus Certificate Service ca@grid.example.org
You may use a command similar to the following:

    cat /tmp/examplegrid/hostcert_request.pem | mail ca@grid.example.org

Only use the above if this machine can send AND receive e-mail. If not, please mail using some other method.

Your certificate will be mailed to you within two working days.
If you receive no response, contact Globus Certificate Service at ca@grid.example.org
Limitations

Only supports PEM-encoded keys, certificates and certificate requests.
Name

grid-default-ca -- Set the default CA to use for certificate requests

grid-default-ca [-help] [-list] [-ca CA-HASH] [-dir SECURITY-DIRECTORY]

Description

The grid-default-ca program sets the default CA used by grid-cert-request. Based on the default CA choice, grid-cert-request will create a certificate request that matches the CA’s naming policies.

If the -ca option is not provided on the command-line, grid-default-ca will display a list of available Certificate Authorities and prompt the user to choose one.

The full set of command-line options to grid-default-ca are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help</td>
<td>Display a help message and exit</td>
</tr>
<tr>
<td>-list</td>
<td>List the available CAs but do not alter the default</td>
</tr>
<tr>
<td>-ca CA-HASH</td>
<td>Select the default CA whose subject name hash matches CA-HASH.</td>
</tr>
<tr>
<td>-dir SECURITY-DIRECTORY</td>
<td>Search SECURITY-DIRECTORY for additional CA certificates.</td>
</tr>
</tbody>
</table>

Examples

Show what certificate authorities are in the trusted cert directory:

% grid-default-ca -list

The available CA configurations installed on this host are:

Directory: /etc/grid-security/certificates

1) 1c3f2ca8 - /DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids CA 1
2) 3d8e6ce8 - /O=Grid/CN=Example CA
3) 6349a761 - /O=DOE Science Grid/OU=Certificate Authorities/CN=Certificate Manager
4) b38b4d8c - /C=US/O=Globus Alliance/CN=Globus Certificate Service

The default CA is: /C=US/O=Globus Alliance/CN=Globus Certificate Service
Location: /etc/grid-security/certificates/b38b4d8c.0

Change the default CA to be DOEGrids CA 1:

% grid-default-ca

The available CA configurations installed on this host are:

Directory: /etc/grid-security/certificates
1) 1c3f2ca8 - /DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids CA 1
2) 3d8e6ce8 - /O=Grid/CN=Example CA
3) 6349a761 - /O=DOE Science Grid/OU=Certificate Authorities/CN=Certificate Manager
4) b38b4d8c - /C=US/O=Globus Alliance/CN=Globus Certificate Service

The default CA is: /C=US/O=Globus Alliance/CN=Globus Certificate Service
Location: /etc/grid-security/certificates/b38b4d8c.0

Enter the index number of the CA to set as the default [q to quit]: 1

setting the default CA to: /DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids CA 1

linking /etc/grid-security/certificates/grid-security.conf.1c3f2ca8 to /etc/grid-security/grid-security.conf

linking /etc/grid-security/certificates/globus-host-ssl.conf.1c3f2ca8 to /etc/grid-security/globus-host-ssl.conf

linking /etc/grid-security/certificates/globus-user-ssl.conf.1c3f2ca8 to /etc/grid-security/globus-user-ssl.conf

...done.

**Limitations**

Displays all CAs in the output, even those where the globus-user-ssl.conf and globus-host-ssl.conf files are not installed in the trusted certificate directory. If one of those is chosen, grid-default-ca displays an error and exits.
Name

grid-change-pass-phrase -- Change the pass phrase on a private key

grid-change-pass-phrase

Tool description

grid-change-pass-phrase allows one to change the passphrase that protects the private key.

Command syntax

grid-change-pass-phrase [-help] [-version] [-file private_key_file]

Changes the passphrase that protects the private key. Note that this command will work even if the original key is not password protected. If the -file argument is not given, the default location of the file containing the private key is assumed:

- The location pointed to by X509_USER_KEY
- If X509_USER_KEY not set, $HOME/.globus/userkey.pem

Options

Table 1. Command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>help, -usage</td>
<td>Displays usage.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-file location</td>
<td>Changes the passphrase on the key stored in the file at the non-standard location 'location'.</td>
</tr>
</tbody>
</table>

Limitations

Nothing applicable
Name

grid-proxy-init -- Generate a new proxy certificate

grid-proxy-init

Tool description

grid-proxy-init generates X.509 proxy certificates.

By default, this command generates RFC 3820\(^1\) Proxy Certificates.

There are also options available for generating other types of proxy certificates, including limited, independent and legacy. For more information about proxy certificate types and their compatibility in GT, see [http://dev.globus.org/wiki/Security/ProxyCertTypes](http://dev.globus.org/wiki/Security/ProxyCertTypes).

Command syntax

```
grid-proxy-init [-help][-pwstdin][-limited][-valid H:M] ...
```

---

\(^1\) [http://www.ietf.org/rfc/rfc3820.txt](http://www.ietf.org/rfc/rfc3820.txt)
Options

Table 2. Command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help, -usage</td>
<td>Displays usage.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-debug</td>
<td>Enables extra debug output.</td>
</tr>
<tr>
<td>-q</td>
<td>Quiet mode, minimal output.</td>
</tr>
<tr>
<td>-verify</td>
<td>Verifies the certificate to make the proxy for.</td>
</tr>
<tr>
<td>-pwstdin</td>
<td>Allows passphrase from stdin.</td>
</tr>
<tr>
<td>-limited</td>
<td>Creates a limited globus proxy.</td>
</tr>
<tr>
<td>-independent</td>
<td>Creates an independent globus proxy.</td>
</tr>
<tr>
<td>-draft</td>
<td>Creates a draft (GSI-3) proxy.</td>
</tr>
<tr>
<td>-old</td>
<td>Creates a legacy globus proxy.</td>
</tr>
<tr>
<td>-valid &lt;h:m&gt;</td>
<td>Proxy is valid for ( h ) hours and ( m ) minutes (default:12:00).</td>
</tr>
<tr>
<td>-hours &lt;hours&gt;</td>
<td>Deprecated support of hours option.</td>
</tr>
<tr>
<td>-bits &lt;bits&gt;</td>
<td>Number of bits in key {512</td>
</tr>
<tr>
<td>-policy &lt;policyfile&gt;</td>
<td>File containing the policy to store in the ProxyCertInfo extension.</td>
</tr>
<tr>
<td>-pl &lt;oid&gt;, -policy-language &lt;oid&gt;</td>
<td>OID string for the policy language used in the policy file.</td>
</tr>
<tr>
<td>-path-length &lt;l&gt;</td>
<td>Allows a chain of at most 1 proxies to be generated from this one.</td>
</tr>
<tr>
<td>-cert &lt;certfile&gt;</td>
<td>Non-standard location of user certificate.</td>
</tr>
<tr>
<td>-key &lt;keyfile&gt;</td>
<td>Non-standard location of user key.</td>
</tr>
<tr>
<td>-certdir &lt;certdir&gt;</td>
<td>Non-standard location of trusted cert directory.</td>
</tr>
<tr>
<td>-out &lt;proxyfile&gt;</td>
<td>Non-standard location of new proxy cert.</td>
</tr>
</tbody>
</table>

Creating a Proxy Certificate

Proxies are certificates signed by the user, or by another proxy, that do not require a password to submit a job. They are intended for short-term use, when the user is submitting many jobs and cannot be troubled to repeat his password for every job.

The subject of a proxy certificate is the same as the subject of the certificate that signed it, with /CN=proxy added to the name. The gatekeeper will accept any job requests submitted by the user, as well as any proxies he has created.

Proxies provide a convenient alternative to constantly entering passwords, but are also less secure than the user’s normal security credential. Therefore, they should always be user-readable only, and should be deleted after they are no longer needed (or after they expire).

To create a proxy with the default expiration (12 hours), run the grid-proxy-init program. For example:

% grid-proxy-init

The grid-proxy-init program can also take arguments to specify the expiration and proxy key length. For example:

% grid-proxy-init -hours 8 -bits 512
Limitations

Nothing applicable
Name

grid-proxy-destroy -- Destroy the current proxy certificate (previously created with grid-proxy-init)

grid-proxy-destroy

Tool description

grid-proxy-destroy removes X.509 proxy certificates.

Command syntax

grid-proxy-destroy [-help][-dryrun][-default][-all][--] [file1...]

Options

Table 3. Command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help, -usage</td>
<td>Displays usage.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-debug</td>
<td>Displays debugging information.</td>
</tr>
<tr>
<td>-dryrun</td>
<td>Prints what files would have been destroyed.</td>
</tr>
<tr>
<td>-default</td>
<td>Destroys file at default proxy location.</td>
</tr>
<tr>
<td>-all</td>
<td>Destroys any user (default) and delegated proxies that are found.</td>
</tr>
<tr>
<td>--</td>
<td>Ends processing of options.</td>
</tr>
<tr>
<td>file1 file2 ...</td>
<td>Destroys the files listed.</td>
</tr>
</tbody>
</table>

Limitations

Nothing applicable
Name
grid-proxy-info -- Display information obtained from a proxy certificate

grid-proxy-info

Tool description
grid-proxy-info extracts information from X.509 proxy certificates.

Command syntax
grid-proxy-info [-help][-f proxyfile][-subject][...][-e [-h H][-b B]]

Options
Table 4. Command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help, -usage</td>
<td>Displays usage.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-debug</td>
<td>Displays debugging output.</td>
</tr>
<tr>
<td>-file &lt;proxyfile&gt; (-f)</td>
<td>Non-standard location of proxy.</td>
</tr>
<tr>
<td>[printoptions]</td>
<td>See Table 5, “Print options”.</td>
</tr>
<tr>
<td>-exists [options] (-e)</td>
<td>Determine whether a valid proxy exists. options may contain any validation options described below. If a proxy exists, and meets any criteria defined by the validity options, then grid-proxy-info will terminate with the exit code 0. Otherwise, grid-proxy-info will terminate with the exit code 1. If no validity options are specified, the program will terminate with 0 if a currently-valid proxy file exists.</td>
</tr>
</tbody>
</table>

Table 5. Print options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-subject (-s)</td>
<td>Distinguished name (DN) of the subject.</td>
</tr>
<tr>
<td>-issuer (-i)</td>
<td>DN of the issuer (certificate signer).</td>
</tr>
<tr>
<td>-identity</td>
<td>DN of the identity represented by the proxy.</td>
</tr>
<tr>
<td>-type</td>
<td>Type of proxy (full or limited).</td>
</tr>
<tr>
<td>-timeleft</td>
<td>Time (in seconds) until proxy expires.</td>
</tr>
<tr>
<td>-strength</td>
<td>Key size (in bits).</td>
</tr>
<tr>
<td>-all</td>
<td>All above options in a human readable format.</td>
</tr>
<tr>
<td>-text</td>
<td>All of the certificate.</td>
</tr>
<tr>
<td>-path</td>
<td>Pathname of the proxy file.</td>
</tr>
</tbody>
</table>
**Table 6. Validity options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-valid H:M (-v)</td>
<td>Time requirement for the proxy to be valid.</td>
</tr>
<tr>
<td>-hours H (-h)</td>
<td>Time requirement for the proxy to be valid (deprecated, use -valid instead).</td>
</tr>
<tr>
<td>-bits B (-b)</td>
<td>Strength requirement for the proxy to be valid.</td>
</tr>
</tbody>
</table>

**Limitations**

Nothing applicable
Name

grid-mapfile-add-entry -- Add an entry to a grid map file

grid-mapfile-add-entry

Tool description

grid-mapfile-add-entry adds entries to grid map files.

Command syntax

grid-mapfile-add-entry -dn DN -ln LN [-help] [-d] [-f mapfile FILE]

Options:

Table 7. Command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help, -usage</td>
<td>Displays help.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-dn DN</td>
<td>Distinguished Name (DN) to add. Remember to quote the DN if it contains spaces.</td>
</tr>
<tr>
<td>-ln LN1 [LN2...]</td>
<td>Local login name(s) to which the DN is mapped.</td>
</tr>
<tr>
<td>-dryrun, -d</td>
<td>Shows what would be done but will not add the entry.</td>
</tr>
<tr>
<td>-mapfile FILE, -f FILE</td>
<td>Path of the grid map file to be used.</td>
</tr>
</tbody>
</table>

Limitations

Nothing applicable.
Name
grid-mapfile-check-consistency -- Check the internal consistency of a grid map file

grid-mapfile-check-consistency

Tool description
grid-mapfile-check-consistency checks that the given grid mapfile conforms to the expected format as well as checking for common subject name problems.

Command syntax
grid-mapfile-check-consistency [-help] [-mapfile FILE]

Options:

Table 8. Command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help, -usage</td>
<td>Displays help.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-mapfile FILE, -f FILE</td>
<td>Path of the grid map file to be used.</td>
</tr>
</tbody>
</table>

Limitations
Nothing applicable
**Name**

grid-mapfile-delete-entry -- Delete an entry from a grid map file

grid-mapfile-delete-entry

**Tool description**

grid-mapfile-delete entry deletes a grid map file entry from the given file.

**Command syntax**


**Options:**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help, -usage</td>
<td>Displays help.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-dn &lt;DN&gt;</td>
<td>Distinguished Name (DN) to delete.</td>
</tr>
<tr>
<td>-ln &lt;local name&gt;</td>
<td>Local Login Name (LN) to delete.</td>
</tr>
<tr>
<td>-dryrun, -d</td>
<td>Shows what would be done but will not delete the entry.</td>
</tr>
<tr>
<td>-mapfile file, -f file</td>
<td>Path of the grid map file to be used.</td>
</tr>
</tbody>
</table>

**Limitations**

Nothing applicable.
Chapter 7. Configuring Certificates

This section describes the configuration steps required to:

• determine whether or not to trust certificates issued by a particular Certificate Authority (CA),
• provide appropriate default values for use by the grid-cert-request command, which is used to generate certificates,
• request service certificates, used by services to authenticate themselves to users, and
• specify identity mapping information.

In general, Globus tools will look for a configuration file in a user-specific location first, and in a system-wide location if no user-specific file was found. The configuration commands described here may be run by administrators to create system-wide defaults and by individuals to override those defaults.

1. Configuring Globus to Trust a Particular Certificate Authority

1.1. Trusted certificates directory

The Globus tools will trust certificates issued by a CA if (and only if) it can find information about the CA in the trusted certificates directory.

The trusted certificates directory is located as described below and exists either on a per-machine or on a per-installation basis.

X509_CERT_DIR is the environment variable used to specify the path to the trusted certificates directory. This directory contains information about which CAs are trusted (including the CA certificates themselves) and, in some cases, configuration information used by grid-cert-request to formulate certificate requests. The location of the trusted certificates directory is looked for in the following order:

1. value of the X509_CERT_DIR environment variable
2. $HOME/.globus/certificates
3. /etc/grid-security/certificates exists
4. $GLOBUS_LOCATION/share/certificates

1.2. Trusted certificates files

The following two files must exist in the directory for each trusted CA:

Table 7.1. CA files

| cert_hash.0 | The trusted CA Certificate. |
| cert_hash.signing_policy | A configuration file defining the distinguished names of certificates signed by the CA. |

Non-WS Globus components will honor a certificate only if:
• its CA certificate exists (with the appropriate name) in the TRUSTED_CA directory, and
• the certificate’s distinguished name matches the pattern described in the signing policy file.

1.3. Hash of the CA certificate

The cert_hash that appears in the file names above is the hash of the CA certificate, which can be found by running the command:

$GLOBUS_LOCATION/bin/openssl x509 -hash -noout < ca_certificate

1.4. Creating a signing policy by hand

Some CAs provide tools to install their CA certificates and signing policy files into the trusted certificates directory. You can, however, create a signing policy file by hand; the signing policy file has the following format:

access_id_CA X509 'CA Distinguished Name'
pos_rights globus CA:sign
cond_subjects globus ""Distinguished Name Pattern"

In the above, the CA Distinguished Name is the subject name of the CA certificate, and the Distinguished Name Pattern is a string used to match the distinguished names of certificates granted by the CA.

Some very simple wildcard matching is done: if the Distinguished Name Pattern ends with a '*', then any distinguished name that matches the part of the CA subject name before the '*' is considered a match.

Note: the cond_subjects line may contain a space-separated list of distinguished name patterns.

1.5. Repository of CAs

A repository of CA certificates that are widely used in academic and research settings can be found here¹.

2. Configuring Globus to Create Appropriate Certificate Requests

The grid-cert-request command, which is used to create certificates, uses the following configuration files:

Table 7.2. Certificate request configuration files

<table>
<thead>
<tr>
<th>Configuration file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>globus-user-ssl.conf</td>
<td>Defines the distinguished name to use for a user's certificate request.</td>
</tr>
<tr>
<td></td>
<td>The format is described here².</td>
</tr>
<tr>
<td>globus-host-ssl.conf</td>
<td>Defines the distinguished name for a host (or service) certificate request.</td>
</tr>
<tr>
<td></td>
<td>The format is described here³.</td>
</tr>
<tr>
<td>grid-security.conf</td>
<td>A base configuration file that contains the name and email address for the CA.</td>
</tr>
<tr>
<td>directions</td>
<td>An optional file that may contain directions on using the CA.</td>
</tr>
</tbody>
</table>

¹ https://www.tacar.org/certs.html
² http://www.openssl.org/docs/apps/req.html#CONFIGURATION_FILE_FORMAT
³ http://www.openssl.org/docs/apps/req.html#CONFIGURATION_FILE_FORMAT
Many CAs provide tools to install configuration files with the following names in the Trusted Certificates directory:

- `globus-user-ssl.conf.cert_hash`
- `globus-host-ssl.conf.cert_hash`
- `grid_security.conf.cert_hash`
- `directions.cert_hash`

### 2.1. Creating a certificate request for a specific CA

The command:

```
grid-cert-request -ca cert_hash
```

will create a certificate request based on the specified CA's configuration files.

### 2.2. Listing available CAs

The command:

```
grid-cert-request -ca
```

will list the available CAs and let the user choose which one to create a request for.

### 2.3. Specifying a default CA for certificate requests

The default CA is the CA that will be used for certificate requests if `grid-cert-request` is invoked without the `-ca` flag.

You can specify a default CA by invoking the `grid-default-ca` command (follow the link for examples of using the command).

### 2.4. `directions` file

The `directions` file may contain specific directions on how to use the CA. There are three types of printed messages:

- `REQUEST HEADER`, printed to a certificate request file,
- `USER INSTRUCTIONS`, printed on the screen when one requests a `user certificate`,
- `NONUSER INSTRUCTIONS`, printed on the screen when one requests a certificate for a service.

Each message is delimited from others with lines `----- BEGIN message type TEXT -----` and `----- END message type TEXT -----`. For example, the `directions` file would contain the following lines:

```
----- BEGIN REQUEST HEADER TEXT -----  
This is a Certificate Request file

It should be mailed to ${GSI_CA_EMAIL_ADDR} 
----- END REQUEST HEADER TEXT ----- 
```

If this file does not exist, the default messages are printed.
3. Requesting Service Certificates

Different CAs use different mechanisms for issuing end-user certificates; some use mechanisms that are entirely web-based, while others require you to generate a certificate request and send it to the CA. If you need to create a certificate request for a service certificate, you can do so by running:

```
grid-cert-request -host hostname -service service_name
```

where `hostname` is the fully-qualified name of the host on which the service will be running, and `service_name` is the name of the service. This will create the following three files:

<table>
<thead>
<tr>
<th>File Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRID_SECURITY/service_name/service_name_cert.pem</td>
<td>An empty file. When you receive your actual service certificate from your CA, you should place it in this file.</td>
</tr>
<tr>
<td>GRID_SECURITY/service_name/service_name_cert_request.pem</td>
<td>The certificate request, which you should send to your CA.</td>
</tr>
<tr>
<td>GRID_SECURITY/service_name/service_name_key.pem</td>
<td>The private key associated with your certificate request, encrypted with the pass phrase that you entered when prompted by <code>grid-cert-request</code>.</td>
</tr>
</tbody>
</table>

The `grid-cert-request` command recognizes several other useful options; you can list these with:

```
grid-cert-request -help
```

4. Configuring Credential Mappings

Several Globus services map certificates to local unix usernames to be used with unix services. The default implementation uses a `gridmap` file to map the distinguished name of the identity of the client’s certificate to a local login name. Administrators can modify the contents of the gridmap file to control what certificate identities are allowed to access Globus services, as well as configure, via an environment variable, what gridmap file a particular service uses.

In addition to the identity-based mapping done via the gridmap file, administrators can configure Globus services to use arbitrary mapping functions. These may use other criteria, such as SAML assertions, to map a certificate to a local account, or may map certificates to temporary accounts. Administrators can install different mapping implementations and configure services to use them by creating appropriate configuration files and setting environment variables.

4.1. Configuring Identity Mappings Using `gridmap` Files

Gridmap files contain a database of entries mapping distinguished names to local user names. These may be manipulated by using the following tools.

4.1.1. Adding an entry to a gridmap file

To add an entry to the gridmap file, run:

```
$GLOBUS_LOCATION/sbin/grid-mapfile-add-entry -dn "Distinguished Name" -ln local_name
```
4.1.2. Deleting an entry from a gridmap file

To delete an entry from the gridmap file, run:

```
$GLOBUS_LOCATION/sbin/grid-mapfile-delete-entry \\
-dn "Distinguished Name" \\
-ln local_name
```

4.1.3. Checking consistency of a gridmap file

To check the consistency of the gridmap file, run

```
$GLOBUS_LOCATION/sbin/grid-mapfile-check-consistency
```

4.1.4. Configuring per-service gridmap files

To configure a service to use a particular gridmap file, set the GRIDMAP variable in the service's environment to the path of the gridmap file. In this way, you can grant different access rights to different certificate identities on a per-service basis by setting the GRIDMAP variable in different service environments.

You can use tools described above to operate on different gridmap files by either setting the GRIDMAP environment variable prior to invoking them, or by using the –mapfile command-line option.

For reference, the GSI C code looks for the gridmap in these locations:

Table 7.4. Gridmap File Location Algorithm

<table>
<thead>
<tr>
<th>Location</th>
<th>notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRIDMAP environment variable</td>
<td></td>
</tr>
<tr>
<td>/etc/grid-security/grid-mapfile</td>
<td>Only for services running as root.</td>
</tr>
<tr>
<td>HOME.gridmap</td>
<td>Only for services not running as root.</td>
</tr>
</tbody>
</table>

4.1.5. Gridmap formats

A gridmap line of the form:

"Distinguished Name" local_name

maps the distinguished name Distinguished Name to the local name local_name.

A gridmap line of the form:

"Distinguished Name" local_name1,local_name2

maps Distinguished Name to both local_name1 and local_name2; any number of local user names may occur in the comma-separated local name list.

For more detailed information about the gridmap file see the file description and grammars on dev.globus.org.

---

4 https://dev.globus.org/wiki/Gridmap
4.2. Configuring Alternate Credential Mappings

To use an alternative credential mapping, you create a gsi-authz.conf file containing information about how the mapping functions are called from the authorization library.

To configure a per-service authorization configuration file, set the GSI_AUTHZ_CONF variable to the path to the configuration file in the environment of the service.

For reference, the GSI C code looks for the authorization configuration file in these locations (in the given order):

Table 7.5. Authorization Configuration File Locations

<table>
<thead>
<tr>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSI_AUTHZ_CONF environment variable</td>
</tr>
<tr>
<td>/etc/grid-security/gsi-authz.conf</td>
</tr>
<tr>
<td>GLOBUS_LOCATION/etc/gsi-authz.conf</td>
</tr>
<tr>
<td>HOME/.gsi-authz.conf</td>
</tr>
</tbody>
</table>

4.2.1. Callout File Format

The authorization file defines a set of callouts, one per line. Each callout is defined by an abstract type, library, and symbol separated by whitespace. Comments begin with the # character and continue to the end of line.

Table 7.6. Authorization Configuration File Locations

<table>
<thead>
<tr>
<th>Field</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>abstract type</td>
<td>Type of the callout: globus_mapping is used for credential mapping callouts</td>
</tr>
<tr>
<td>library</td>
<td>Path to the shared object containing the callout implementation. The library name may be a literal filename, or a partial filename to which the compilation flavor of the service is appended to the filename before its extension.</td>
</tr>
<tr>
<td>symbol</td>
<td>The exported symbol containing the entry point to the callout implementation.</td>
</tr>
</tbody>
</table>

Here is a sample gsi-authz.conf file that configures a globus_mapping callout to use the globus_gridmap_callout function in the /usr/local/globus/lib/libglobus_gridmap_callout_gcc32dbg shared object:

```plaintext
# abstract-type library symbol
globus_mapping /opt/globus/lib/libglobus_gridmap_callout_gcc32dbg globus_gridmap_call
```

5. GSI File Permissions Requirements

- **End Entity Certificate (User, Host and Service) Certificates and the GSI Authorization Callout Configuration File:**
  - May not be executable
  - May not be writable by group and other
  - Must be either regular files or soft links
- **Private Keys and Proxy Credentials:**
Configuring Certificates

- Must be owned by the current (effective) user
- May not be executable
- May not be readable by group and other
- May not be writable by group and other
- Must be either regular files or soft links

- CA Certificates, CA Signing Policy Files, the Grid Map File and the GAA Configuration File:
  - Must be either regular files or soft links

- GSI Authorization callout configuration files
  - Must exist
  - Should be world readable
  - Should not be writable by group and other
  - Should be either a regular file or a soft link

- GSI GAA configuration files
  - Must exist
  - Should be world readable
  - Should not be writable by group and other
  - Should be either a regular file or a soft link
Chapter 8. Environment variable interface

1. Environmental Variables for GSI C

1.1. Credentials

Credentials are looked for in the following order:

1. service credential
2. host credential
3. proxy credential
4. user credential

`X509_USER_PROXY` specifies the path to the `proxy credential`. If `X509_USER_PROXY` is not set, the proxy credential is created (by `grid-proxy-init`) and searched for (by client programs) in an operating-system-dependent local temporary file.

`X509_USER_CERT` and `X509_USER_KEY` specify the path to the end entity (user, service, or host) certificate and corresponding `private key`. The paths to the certificate and key files are determined as follows:

For `service credentials`:

1. If `X509_USER_CERT` and `X509_USER_KEY` exist and contain a valid certificate and key, those files are used.
2. Otherwise, if the files `/etc/grid-security/service/servicecert` and `/etc/grid-security/service/servicekey` exist and contain a valid certificate and key, those files are used.
3. Otherwise, if the files `$GLOBUS_LOCATION/etc/grid-security/service/servicecert` and `$GLOBUS_LOCATION/etc/grid-security/service/servicekey` exist and contain a valid certificate and key, those files are used.
4. Otherwise, if the files `service/servicecert` and `service/servicekey` in the user's `.globus` directory exist and contain a valid certificate and key, those files are used.

For `host credentials`:

1. If `X509_USER_CERT` and `X509_USER_KEY` exist and contain a valid certificate and key, those files are used.
2. Otherwise, if the files `/etc/grid-security/hostcert.pem` and `/etc/grid-security/hostkey.pem` exist and contain a valid certificate and key, those files are used.
3. Otherwise, if the files `$GLOBUS_LOCATION/etc/hostcert.pem` and `$GLOBUS_LOCATION/etc/hostkey.pem` exist and contain a valid certificate and key, those files are used.
4. Otherwise, if the files `hostcert.pem` and `hostkey.pem` in the user's `.globus` directory exist and contain a valid certificate and key, those files are used.

For `user credentials`:
If X509_USER_CERT and X509_USER_KEY exist and contain a valid certificate and key, those files are used.

Otherwise, if the files usercert.pem and userkey.pem exist in the user's .globus directory, those files are used.

Otherwise, if a PKCS-12 file called usercred.p12 exists in the user's .globus directory, the certificate and key are read from that file.

### 1.2. Gridmap file

GRIDMAP specifies the path to the grid map file, which is used to map distinguished names (found in certificates) to local names (such as login accounts). The location of the grid map file is determined as follows:

1. If the GRIDMAP environment variable is set, the grid map file location is the value of that environment variable.
2. Otherwise:
   - If the user is root (uid 0), then the grid map file is /etc/grid-security/grid-mapfile.
   - Otherwise, the grid map file is $HOME/.gridmap.

### 1.3. Trusted CAs directory

X509_CERT_DIR is used to specify the path to the trusted certificates directory. This directory contains information about which CAs are trusted (including the CA certificates themselves) and, in some cases, configuration information used by grid-cert-request to formulate certificate requests. The location of the trusted certificates directory is determined as follows:

1. If the X509 CERT_DIR environment variable is set, the trusted certificates directory is the value of that environment variable.
2. Otherwise, if $HOME/.globus/certificates exists, that directory is the trusted certificates directory.
3. Otherwise, if /etc/grid-security/certificates exists, that directory is the trusted certificates directory.
4. Finally, if $GLOBUS_LOCATION/share/certificates exists, then it is the trusted certificates directory.

### 1.4. GSI authorization callout configuration file

GSI_AUTHZ_CONF is used to specify the path to the GSI authorization callout configuration file. This file is used to configure authorization callouts used by both the gridmap and the authorization API. The location of the GSI authorization callout configuration file is determined as follows:

1. If the GSI_AUTHZ_CONF environment variable is set, the authorization callout configuration file location is the value of that environment variable.
2. Otherwise, if /etc/grid-security/gsi-authz.conf exists, then this file is used.
3. Otherwise, if $GLOBUS_LOCATION/etc/gsi-authz.conf exists, then this file is used.
4. Finally, if $HOME/.gsi-authz.conf exists, then this file is used.
1.5. **GAA (Generic Authorization and Access control) configuration file**

GSI_GAA_CONF is used to specify the path to the GSI GAA configuration file. This file is used to configure policy language specific plugins to the GAA-API. The location of the GSI GAA configuration file is determined as follows:

1. If the GSI_GAA_CONF environment variable is set, the GAA configuration file location is the value of this environment variable.
2. Otherwise, if /etc/grid-security/gsi-gaa.conf exists, then this file is used.
3. Otherwise, if $GLOBUS_LOCATION/etc/gsi-gaa.conf exists, then this file is used.
4. Finally, if $HOME/.gsi-gaa.conf exists, then this file is used.

1.6. **Grid security directory**

GRID_SECURITY_DIR specifies a path to a directory containing configuration files that specify default values to be placed in certificate requests. This environment variable is used only by the grid-cert-request and grid-default-ca commands.

The location of the grid security directory is determined as follows:

1. If the GRID_SECURITY_DIR environment variable is set, the grid security directory is the value of that environment variable.
2. If the configuration files exist in /etc/grid-security, the grid security directory is that directory.
3. If the configuration files exist in $GLOBUS_LOCATION/etc, the grid security directory is that directory.

1.7. **Using TLS**

GLOBUS_GSSAPI_FORCE_TLS specifies whether to use TLS by default when establishing a security context. The default behavior if this is not set is to use SSLv3.

1.8. **Name Comparisons**

GLOBUS_GSSAPI_NAME_COMPATIBILITY specifies what name matching algorithms are supported by GSSAPI for mutual authentication and gss_compare_name. This variable may be set to any of the following values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRICT_GT2</td>
<td>Strictly backward-compatible with GT 2.0 name matching. X.509 subjectAltName values are ignored. Names with hyphens are treated as wildcards as described in the security considerations documentation. Name matching will rely on canonical host name associated with connection IP addresses.</td>
</tr>
<tr>
<td>STRICT_RFC2818</td>
<td>Support RFC 2818 server identity processing. Hyphen characters are treated as normal part of a host name. DNSName and IPAddress subjectAltName extensions are matched against the host and port passed to GSSAPI. If subjectAltName is present, X.509 SubjectName is ignored.</td>
</tr>
</tbody>
</table>

1 http://www.ietf.org/rfc/rfc2818.txt
### HYBRID

Support a hybrid of the two previous name matching algorithms, liberally matching both hyphen wildcards, canonical names associated with IP addresses, and subjectAlt-Name extensions.

If this variable is not set, the **HYBRID** behavior is used.
Chapter 9. Debugging

For information about system administrator logs, see Debugging in the GSI C Admin Guide.
Chapter 10. Troubleshooting

For a list of common errors in GT, see Error Codes.

1. Credential Troubleshooting

1.1. Credential Errors

The following are some common problems that may cause clients or servers to report that credentials are invalid:

For a list of common errors in GT, see Error Codes.
### Table 10.1. Credential Errors

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Definition</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your proxy credential may have expired</td>
<td>Your proxy credential may have expired.</td>
<td>Use <code>grid-proxy-info</code> to check whether the proxy credential has actually expired. If it has, generate a new proxy with <code>grid-proxy-init</code>.</td>
</tr>
<tr>
<td>The system clock on either the local or remote system is wrong.</td>
<td>This may cause the server or client to conclude that a credential has expired.</td>
<td>Check the system clocks on the local and remote system.</td>
</tr>
<tr>
<td>Your end-user certificate may have expired</td>
<td>Your end-user certificate may have expired.</td>
<td>Use <code>grid-cert-info</code> to check your certificate's expiration date. If it has expired, follow your CA's procedures to get a new one.</td>
</tr>
<tr>
<td>The permissions may be wrong on your proxy file</td>
<td>If the permissions on your proxy file are too lax (for example, if others can read your proxy file), Globus Toolkit clients will not use that file to authenticate.</td>
<td>You can &quot;fix&quot; this problem by changing the permissions on the file or by destroying it (with <code>grid-proxy-destroy</code>) and creating a new one (with <code>grid-proxy-init</code>). <strong>Important:</strong> However, it is still possible that someone else has made a copy of that file during the time that the permissions were wrong. In that case, they will be able to impersonate you until the proxy file expires or your permissions or end-user certificate are revoked, whichever happens first.</td>
</tr>
<tr>
<td>The permissions may be wrong on your private key file</td>
<td>If the permissions on your end user certificate private key file are too lax (for example, if others can read the file), <code>grid-proxy-init</code> will refuse to create a proxy certificate.</td>
<td>You can &quot;fix&quot; this by changing the permissions on the private key file. <strong>Important:</strong> However, you will still have a much more serious problem: it is possible that someone has made a copy of your private key file. Although this file is encrypted, it is possible that someone will be able to decrypt the private key, at which point they will be able to impersonate you as long as your end user certificate is valid. You should contact your CA to have your end-user certificate revoked and get a new one.</td>
</tr>
<tr>
<td>The remote system may not trust your CA</td>
<td>The remote system may not trust your CA</td>
<td>Verify that the remote system is configured to trust the CA that issued your end-entity certificate. See Installing GT 5.0.0 for details.</td>
</tr>
<tr>
<td>You may not trust the remote system's CA</td>
<td>You may not trust the remote system's CA</td>
<td>Verify that your system is configured to trust the remote CA (or that your environment is set up to trust the remote CA). See Installing GT 5.0.0 for details.</td>
</tr>
<tr>
<td>There may be something wrong with the remote service's credentials</td>
<td>There may be something wrong with the remote service's credentials</td>
<td>It is sometimes difficult to distinguish between errors reported by the remote service regarding your credentials and errors reported by the client interface regarding the remote service's credentials. If you cannot find anything wrong with your credentials, check for the same conditions on the remote system (or ask a remote administrator to do so).</td>
</tr>
</tbody>
</table>
1.2. Some tools to validate certificate setup

1.2.1. grid-cert-diagnostics

The `grid-cert-diagnostics` program checks prints diagnostics about the user's certificates, and host security environment.

```
% grid-cert-diagnostics -p
```

1.2.2. Check that the user certificate is valid

```
openssl verify -CApath /etc/grid-security/certificates
   -purpose sslclient ~/.globus/usercert.pem
```

1.2.3. Connect to the server using s_client

```
openssl s_client -ssl3 -cert ~/.globus/usercert.pem -key ~/.globus/userkey.pem -CApath /etc/grid-security/certificates
   -connect <host:port>
```

Here `<host:port>` denotes the server and port you connect to.

If it prints an error and puts you back at the command prompt, then it typically means that the server has closed the connection, i.e. that the server was not happy with the client's certificate and verification. Check the SSL log on the server.

If the command "hangs" then it has actually opened a telnet style (but secure) socket, and you can "talk" to the server.

You should be able to scroll up and see the subject names of the server's verification chain:

- `depth=2 /DC=net/DC=ES/O=ESnet/OU=Certificate Authorities/CN=ESnet Root CA 1
  verify return:1`
- `depth=1 /DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids CA 1
  verify return:1`
- `depth=0 /DC=org/DC=doegrids/OU=Services/CN=wiggum.mcs.anl.gov
  verify return:1`

In this case, there were no errors. Errors would give you an extra line next to the subject name of the certificate that caused the error.

1.2.4. Check that the server certificate is valid

Requires root login on server:

```
openssl verify -CApath /etc/grid-security/certificates -purpose sslserver
   /etc/grid-security/hostcert.pem
```
2. Grid map Troubleshooting

2.1. Grid map errors

The following are some common problems that may cause clients or servers to report that user are not authorized:

For a list of common errors in GT, see Error Codes.

Table 10.2. Gridmap Errors

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Definition</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The content of the grid map file does not conform to the expected format</td>
<td>The content of the grid map file does not conform to the expected format</td>
<td>Run grid-mapfile-check-consistency to make sure that your gridmap file conforms to the expected format.</td>
</tr>
<tr>
<td>The grid map file does not contain a entry for your DN</td>
<td>The grid map file does not contain a entry for your DN</td>
<td>Use grid-mapfile-add-entry to add the relevant entry.</td>
</tr>
</tbody>
</table>
Chapter 11. Related Documentation

- RFC 3820\(^1\) Proxy Certificates
- RFC 2744\(^2\) GSSAPI: C-bindings
- RFC 2743\(^3\) GSSAPI
- GSSAPI Extensions\(^4\)
- RFC 2246\(^5\) TLS
- Grid Security Infrastructure Message Specification\(^6\)

---

\(^1\) http://www.faqs.org/rfcs/rfc3820.html
\(^2\) http://www.faqs.org/rfcs/rfc2744.html
\(^3\) http://www.faqs.org/rfcs/rfc2743.html
\(^5\) http://www.faqs.org/rfc/rfc2246.html
\(^6\) http://www.globus.org/toolkit/docs/3.0/gsi/GSI-message-specification-02.doc
Glossary

C

Certificate Authority (CA) An entity that issues certificates.

CA Certificate The CA’s certificate. This certificate is used to verify signature on certificates issued by the CA. GSI typically stores a given CA certificate in /etc/grid-security/certificates/<hash>.0, where <hash> is the hash code of the CA identity.

CA Signing Policy The CA signing policy is used to place constraints on the information you trust a given CA to bind to public keys. Specifically it constrains the identities a CA is trusted to assert in a certificate. In GSI the signing policy for a given CA can typically be found in /etc/grid-security/certificates/<hash>.signing_policy, where <hash> is the hash code of the CA identity.

E

End Entity Certificate (EEC) A certificate belonging to a non-CA entity, e.g. you, me or the computer on your desk.

G

GAA configuration file A file that configures the Generic Authorization and Access control GAA libraries. When using GSI, this file is typically found in /etc/grid-security/gsi-gaa.conf.

grid map file A file containing entries mapping certificate subjects to local user names. This file can also serve as a access control list for GSI enabled services and is typically found in /etc/grid-security/grid-mapfile. For more information see the Gridmap section here.

grid security directory The directory containing GSI configuration files such as the GSI authorization callout configuration and GAA configuration files. Typically this directory is /etc/grid-security. For more information see this.

GSI authorization callout configuration file A file that configures authorization callouts to be used for mapping and authorization in GSI enabled services. When using GSI this file is typically found in /etc/grid-security/gsi-authz.conf.

H

host certificate An EEC belonging to a host. When using GSI this certificate is typically stored in /etc/grid-security/hostcert.pem. For more information on possible host certificate locations see the GSI C Developer’s Guide.

host credentials The combination of a host certificate and its corresponding private key.
### Glossary

**P**

**private key**
The private part of a key pair. Depending on the type of certificate the key corresponds to it may typically be found in `$HOME/.globus/userkey.pem` (for user certificates), `/etc/grid-security/hostkey.pem` (for host certificates) or `/etc/grid-security/<service>/key.pem` (for service certificates).

For more information on possible private key locations see [this](#).

**proxy certificate**
A short lived certificate issued using a EEC. A proxy certificate typically has the same effective subject as the EEC that issued it and can thus be used in its place. GSI uses proxy certificates for single sign on and delegation of rights to other entities.

For more information about types of proxy certificates and their compatibility in different versions of GT, see [http://dev.globus.org/wiki/Security/ProxyCertTypes](http://dev.globus.org/wiki/Security/ProxyCertTypes).

**proxy credentials**
The combination of a proxy certificate and its corresponding private key. GSI typically stores proxy credentials in `/tmp/x509up_u<uid>` , where `<uid>` is the user id of the proxy owner.

**S**

**service certificate**
A EEC for a specific service (e.g. FTP or LDAP). When using GSI this certificate is typically stored in `/etc/grid-security/<service>/cert.pem`. For more information on possible service certificate locations, see [this](#).

**service credentials**
The combination of a service certificate and its corresponding private key.

**U**

**user certificate**
A EEC belonging to a user. When using GSI, this certificate is typically stored in `$HOME/.globus/usercert.pem`. For more information on possible user certificate locations, see [this](#).

**user credentials**
The combination of a user certificate and its corresponding private key.