

GT4: Security: GSI C User's Guide

DRAFT

GT4: Security: GSI C User's Guide

Introduction

Authentication in the Globus Toolkit is based on X.509 certificates. This document describes how to acquire and use the certificates that you will need to authenticate yourself to Globus services.

DRAFT

Table of Contents

1. Usage scenarios	1
1. Basic procedure for using GSI C	1
I. GSI Commands	2
grid-cert-info	3
grid-cert-request	5
grid-default-ca	8
grid-change-pass-phrase	9
grid-proxy-init	10
grid-proxy-destroy	13
grid-proxy-info	14
grid-mapfile-add-entry	16
grid-mapfile-check-consistency	17
grid-mapfile-delete-entry	18
2. Troubleshooting	19
1. Credential Troubleshooting	19
2. Grid map Troubleshooting	21
Glossary	23

List of Tables

1. Command line options	8
2. Command line options	9
3. Command line options	11
4. Command line options	13
5. Command line options	14
6. Print options	14
7. Validity options	14
8. Command line options	16
9. Command line options	17
10. Command line options	18
2.1. Credential Errors	20
2.2. Gridmap Errors	22

DRAFT

Chapter 1. Usage scenarios

1. Basic procedure for using GSI C

In most cases, an individual will do the following:

- Acquire a *user certificate* from a certification authority (CA) with `grid-cert-request`. This certificate will typically be valid for a year or more and will be stored in a file in the individual's home directory.

It is important to keep in mind when your cert will expire - after your user certificate expires, you may not be able to use secure services in GT!

- Use the end-user certificate to create a *proxy certificate* using `grid-proxy-init`. This will be used to authenticate the individual to grid services. Proxy certificates typically have a much shorter lifetime than end-user certificates (usually 12 hours). Once your proxy certificate expires, simply rerun **grid-proxy-init**.

GSI Commands

DRAFT

Name

grid-cert-info -- Display certificate information

```
grid-cert-info [-help] [-version]
[-file CERTIFICATE-FILENAME]
[-all] [-subject] [-issuer] [-issuerhash] [-startdate] [-enddate]
```

Description

The **grid-cert-info** displays information from a user's credential, or from any X.509 certificate if the `-file CERTIFICATE-FILENAME` 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:

<code>-help</code>	Print help information and exit
<code>-version</code>	Print version information and exit
<code>-file CERTIFICATE-FILENAME</code>	Read credential from <code>CERTIFICATE-FILENAME</code> instead of the default location. The file must have a <code>.pem</code> or <code>.p12</code> extension.
<code>-all</code>	Print all information from the certificate. This is the default unless any of the following options are given.
<code>-subject</code>	Print the subject name of the certificate.
<code>-issuer</code>	Print the subject name of the issuer of the certificate. This is the subject name of the <i>Certificate Authority</i> which signed the certificate.
<code>-issuerhash</code>	Print the hash of the name of the issuer of the certificate. This is the hash of the Certificate Authority which signed the certificate.
<code>-startdate</code>	Print the date and time from which the certificate is valid
<code>-enddate</code>	Print the date and time when the certificate expires.

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.

DRAFT

Name

grid-cert-request -- Create a certificate request

```
grid-cert-request [-help] [-version] [-verbose] [-force]
[-commonname NAME] [-service SERVICE] [-host FQDN] [-interactive]
[-dir DIRECTORY] [-prefix PREFIX] [-ca [HASH]] [-nopw]
```

Description

grid-cert-request generates a public/private key pair and 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:

-help	Print help information and exit
-version	Print version information and exit
-verbose	Don't clear screen after running OpenSSL
-force	Overwrite an existing certificate request if present.
-commonname <i>NAME</i>	Construct a subject name with <i>NAME</i> 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 for a name.
-service <i>SERVICE</i>	Construct a subject name with the common name constructed from the <i>SERVICE</i> name and the hostname joined by the / character. The <i>-service</i> requires that the <i>-host</i> option also be used. The private key created for a service certificate request is not encrypted.
-host <i>FQDN</i>	Construct a subject name with <i>FQDN</i> as the name of the host. This must be a fully-qualified name in dotted string notation (e.g. <i>grid.example.org</i>). If no service is specified by the <i>-service</i> option, the subject name will be <i>host/FQDN</i> . The private key created for a host certificate request is not encrypted. By default the host certificate request and key are created in <i>/etc/grid-security</i> .
-interactive	Interactively prompt for the components of the certificate subject name.
-dir <i>DIRECTORY</i>	Write the certificate request and key to <i>DIRECTORY</i> , creating it if the directory does not exist. By default, the certificate request and key are placed in <i>\$HOME/.globus</i>
-prefix <i>PREFIX</i>	Prepend the string <i>PREFIX</i> to the certificate, key, and request filenames. The default prefix is <i>user</i> for user certificates and <i>host</i> for host certificates.
-ca <i>HASH</i>	Choose a non-default Certificate Authority configuration to construct the certificate request. If <i>HASH</i> 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.
-nopw	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

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

Tool description

grid-default-ca allows the setting of the default CA to be used by tools such as grid-cert-request.

Command syntax

```
grid-default-ca [-help] [ options ...]
```

Options:

Table 1. Command line options

-help	Displays this message.
-dir <dir_name>	The security config directory (defaults to /etc/grid-security/).
-list	Lists the available CAs to use and the current default.
-ca <ca hash>	Sets the default CA non-interactively.

Limitations

Nothing applicable

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 2. Command line options

help, -usage	Displays usage.
-version	Displays version.
-file location	Changes the passphrase on the key stored in the file at the non-standard location 'location'.

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](http://www.ietf.org/rfc/rfc3820.txt)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>.

Command syntax

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

¹ <http://www.ietf.org/rfc/rfc3820.txt>

Options

Table 3. Command line options

-help, -usage	Displays usage.
-version	Displays version.
-debug	Enables extra debug output.
-q	Quiet mode, minimal output.
-verify	Verifies the certificate to make the proxy for.
-pwstdin	Allows passphrase from stdin.
-limited	Creates a limited globus proxy.
-independent	Creates an independent globus proxy.
-draft	Creates a draft (GSI-3) proxy.
-old	Creates a legacy globus proxy.
-valid <h:m>	Proxy is valid for <i>h</i> hours and <i>m</i> minutes (default:12:00).
-hours <hours>	Deprecated support of hours option.
-bits <bits>	Number of bits in key {512 1024 2048 4096}.
-policy <policyfile>	File containing the policy to store in the ProxyCertInfo extension.
-pl <oid>, -policy-language <oid>	OID string for the policy language used in the policy file.
-path-length <l>	Allows a chain of at most 1 proxies to be generated from this one.
-cert <certfile>	Non-standard location of user certificate.
-key <keyfile>	Non-standard location of user key.
-certdir <certdir>	Non-standard location of trusted cert directory.
-out <proxyfile>	Non-standard location of new proxy cert.

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

DRAFT

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 4. Command line options

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

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 5. Command line options

-help, -usage	Displays usage.
-version	Displays version.
-debug	Displays debugging output.
-file <proxyfile> (-f)	Non-standard location of proxy.
[printoptions]	See Table 6, “Print options”.
-exists [options] (-e)	If a valid proxy exists, 1 otherwise. [FIXME this entry is a bit confusing] If none of the following options are given to -exists, H = B = 0 are assumed. See Table 7, “Validity options”.

Table 6. Print options

-subject (-s)	Distinguished name (DN) of the subject.
-issuer (-i)	DN of the issuer (certificate signer).
-identity	DN of the identity represented by the proxy.
-type	Type of proxy (full or limited).
-timeleft	Time (in seconds) until proxy expires.
-strength	Key size (in bits).
-all	All above options in a human readable format.
-text	All of the certificate.
-path	Pathname of the proxy file.

Table 7. Validity options

-valid H:M (-v)	Time requirement for the proxy to be valid.
-hours H (-h)	Time requirement for the proxy to be valid (deprecated, use -valid instead).
-bits B (-b)	Strength requirement for the proxy to be valid.

Limitations

Nothing applicable

DRAFT

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 8. Command line options

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

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 9. Command line options

-help, -usage	Displays help.
-version	Displays version.
-mapfile FILE, -f FILE	Path of the grid map file to be used.

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

grid-mapfile-delete-entry [-help] [-dn <DN>] [-ln <local name>] [-d] [-f file]

Options:

Table 10. Command line options

-help, -usage	Displays help.
-version	Displays version.
-dn <DN>	Distinguished Name (DN) to delete.
-ln <local name>	Local Login Name (LN) to delete.
-dryrun, -d	Shows what would be done but will not delete the entry.
-mapfile file, -f file	Path of the grid map file to be used.

Limitations

Nothing applicable.

Chapter 2. Troubleshooting

The following includes common errors for credentials and gridmap files. For information about system administrator logs, see [Chapter 4, Debugging](#) in the GSI C Admin Guide.

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](#).

DRAFT

Table 2.1. Credential Errors

Error Code	Definition	Possible Solutions
Your proxy credential may have expired	Your proxy credential may have expired.	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> .
The system clock on either the local or remote system is wrong.	This may cause the server or client to conclude that a credential has expired.	Check the system clocks on the local and remote system.
Your end-user certificate may have expired	Your end-user certificate may have expired	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.
The permissions may be wrong on your proxy file	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.	You can "fix" 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>). Important: 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.
The permissions may be wrong on your private key file	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.	You can "fix" this by changing the permissions on the private key file. Important: 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.
The remote system may not trust your CA	The remote system may not trust your CA	Verify that the remote system is configured to trust the CA that issued your end-entity certificate. See Installing GT 4.2.0 for details.
You may not trust the remote system's CA	You may not trust the remote system's CA	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 4.2.0 for details.
There may be something wrong with the remote service's credentials	There may be something wrong with the remote service's credentials	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).

1.2. Some tools to validate certificate setup

1.2.1. Check that the user certificate is valid

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

1.2.2. 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.

1.2.3. 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 2.2. Gridmap Errors

Error Code	Definition	Possible Solutions
The content of the grid map file does not conform to the expected format	The content of the grid map file does not conform to the expected format	Run grid-mapfile-check-consistency to make sure that your gridmap file conforms to the expected format.
The grid map file does not contain a entry for your DN	The grid map file does not contain a entry for your DN	Use grid-mapfile-add-entry to add the relevant entry.

DRAFT

Glossary

some terms not in the docs but wanted in glossary: [scheduler](#)

C

Certificate Authority (CA) An entity that issues certificates. [fixme - flesh out]

G

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](#).

P

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>.

S

scheduler Term used to describe a job scheduler mechanism to which GRAM interfaces. It is a networked system for submitting, controlling, and monitoring the workload of batch jobs in one or more computers. The jobs or tasks are scheduled for execution at a time chosen by the subsystem according to an available policy and availability of resources. Popular job schedulers include Portable Batch System (PBS), Platform LSF, and IBM LoadLeveler.

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](#).