

## **GT 4.2.0 GSI C Public Interfaces**

DRAFT

## GT 4.2.0 GSI C Public Interfaces

DRAFT

---

# Table of Contents

1. APIs .....	1
2. Protocol Specifications .....	3
1. GSI Message Specification .....	3
I. GSI Commands .....	4
grid-cert-info .....	5
grid-cert-request .....	7
grid-default-ca .....	10
grid-change-pass-phrase .....	11
grid-proxy-init .....	12
grid-proxy-destroy .....	15
grid-proxy-info .....	16
grid-mapfile-add-entry .....	18
grid-mapfile-check-consistency .....	19
grid-mapfile-delete-entry .....	20
3. Configuring Certificates .....	21
1. Configuring Globus to Trust a Particular Certificate Authority .....	21
2. Configuring Globus to Create Appropriate Certificate Requests .....	22
3. Requesting Service Certificates .....	24
4. Specifying Identity Mapping Information (gridmap file) .....	25
5. GSI File Permissions Requirements .....	26
4. Environment variable interface .....	27
1. Environmental Variables for GSI C .....	27
A. Errors .....	30
Glossary .....	33

## List of Tables

1. Command line options .....	10
2. Command line options .....	11
3. Command line options .....	13
4. Command line options .....	15
5. Command line options .....	16
6. Print options .....	16
7. Validity options .....	16
8. Command line options .....	18
9. Command line options .....	19
10. Command line options .....	20
3.1. CA files .....	21
3.2. Certificate request configuration files .....	23
3.3. Certificate request files .....	24
A.1. Credential Errors .....	31
A.2. Gridmap Errors .....	32

# Chapter 1. APIs

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

- [gaa\\_core](#)<sup>1</sup> [no frames<sup>2</sup>]
- [gaa\\_gss\\_generic](#)<sup>3</sup> [no frames<sup>4</sup>]
- [gaa\\_plugin](#)<sup>5</sup> [no frames<sup>6</sup>]
- [globus\\_authz](#)<sup>7</sup> [no frames<sup>8</sup>]
- [globus\\_authz\\_callout\\_error](#)<sup>9</sup> [no frames<sup>10</sup>]
- [globus\\_gridmap\\_callout\\_error](#)<sup>11</sup> [no frames<sup>12</sup>]
- [globus\\_gsi\\_callback](#)<sup>13</sup> [no frames<sup>14</sup>]
- [globus\\_gsi\\_cert\\_utils](#)<sup>15</sup> [no frames<sup>16</sup>]
- [globus\\_gsi\\_credential](#)<sup>17</sup> [no frames<sup>18</sup>]
- [globus\\_gsi\\_openssl\\_error](#)<sup>19</sup> [no frames<sup>20</sup>]
- [globus\\_gsi\\_proxy\\_core](#)<sup>21</sup> [no frames<sup>22</sup>]
- [globus\\_gsi\\_proxy\\_ssl](#)<sup>23</sup> [no frames<sup>24</sup>]
- [globus\\_gsi\\_sysconfig](#)<sup>25</sup> [no frames<sup>26</sup>]
- [globus\\_gss\\_assist](#)<sup>27</sup> [no frames<sup>28</sup>]

---

<sup>1</sup> [http://www.globus.org/api/c-globus-4.0/gaa\\_core/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/gaa_core/html/index.html#_top)

<sup>2</sup> [http://www.globus.org/api/c-globus-4.0/gaa\\_core/html/main.html#\\_top](http://www.globus.org/api/c-globus-4.0/gaa_core/html/main.html#_top)

<sup>3</sup> [http://www.globus.org/api/c-globus-4.0/gaa\\_gss\\_generic/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/gaa_gss_generic/html/index.html#_top)

<sup>4</sup> [http://www.globus.org/api/c-globus-4.0/gaa\\_gss\\_generic/html/main.html#\\_top](http://www.globus.org/api/c-globus-4.0/gaa_gss_generic/html/main.html#_top)

<sup>5</sup> [http://www.globus.org/api/c-globus-4.0/gaa\\_plugin/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/gaa_plugin/html/index.html#_top)

<sup>6</sup> [http://www.globus.org/api/c-globus-4.0/gaa\\_plugin/html/main.html#\\_top](http://www.globus.org/api/c-globus-4.0/gaa_plugin/html/main.html#_top)

<sup>7</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_authz/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_authz/html/index.html#_top)

<sup>8</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_authz/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_authz/html/main.html)

<sup>9</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_authz\\_callout\\_error/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_authz_callout_error/html/index.html#_top)

<sup>10</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_authz\\_callout\\_error/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_authz_callout_error/html/main.html)

<sup>11</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gridmap\\_callout\\_error/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_gridmap_callout_error/html/index.html#_top)

<sup>12</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gridmap\\_callout\\_error/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_gridmap_callout_error/html/main.html)

<sup>13</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_callback/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_gsi_callback/html/index.html#_top)

<sup>14</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_callback/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_gsi_callback/html/main.html)

<sup>15</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_cert\\_utils/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_gsi_cert_utils/html/index.html#_top)

<sup>16</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_cert\\_utils/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_gsi_cert_utils/html/main.html)

<sup>17</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_credential/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_gsi_credential/html/index.html#_top)

<sup>18</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_credential/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_gsi_credential/html/main.html)

<sup>19</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_openssl\\_error/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_gsi_openssl_error/html/index.html#_top)

<sup>20</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_openssl\\_error/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_gsi_openssl_error/html/main.html)

<sup>21</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_proxy\\_core/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_gsi_proxy_core/html/index.html#_top)

<sup>22</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_proxy\\_core/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_gsi_proxy_core/html/main.html)

<sup>23</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_proxy\\_ssl/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_gsi_proxy_ssl/html/index.html#_top)

<sup>24</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_proxy\\_ssl/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_gsi_proxy_ssl/html/main.html)

<sup>25</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_sysconfig/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_gsi_sysconfig/html/index.html#_top)

<sup>26</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gsi\\_sysconfig/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_gsi_sysconfig/html/main.html)

<sup>27</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gss\\_assist/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_gss_assist/html/index.html#_top)

<sup>28</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gss\\_assist/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_gss_assist/html/main.html)

- [globus\\_gssapi\\_gsi](#)<sup>29</sup> [no frames<sup>30</sup>]
- [globus\\_openssl\\_module](#)<sup>31</sup> [no frames<sup>32</sup>]
- [gssapi\\_error](#)<sup>33</sup> [no frames<sup>34</sup>]

For information on the internationalization API, see the [CCommon Libraries Public Interface](#).

---

<sup>29</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gssapi\\_gsi/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_gssapi_gsi/html/index.html#_top)

<sup>30</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_gssapi\\_gsi/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_gssapi_gsi/html/main.html)

<sup>31</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_openssl\\_module/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/globus_openssl_module/html/index.html#_top)

<sup>32</sup> [http://www.globus.org/api/c-globus-4.0/globus\\_openssl\\_module/html/main.html](http://www.globus.org/api/c-globus-4.0/globus_openssl_module/html/main.html)

<sup>33</sup> [http://www.globus.org/api/c-globus-4.0/gssapi\\_error/html/index.html#\\_top](http://www.globus.org/api/c-globus-4.0/gssapi_error/html/index.html#_top)

<sup>34</sup> [http://www.globus.org/api/c-globus-4.0/gssapi\\_error/html/main.html](http://www.globus.org/api/c-globus-4.0/gssapi_error/html/main.html)

# Chapter 2. 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 [here](#)<sup>1</sup>.

DRAFT

---

<sup>1</sup> ../GSI-message-specification-02.doc

# 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 <b>finger</b> program. If that fails, <b>grid-cert-request</b> 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 <b>grid-cert-request</b> 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)<sup>1</sup> 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] ...
```

---

<sup>1</sup> <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 3. 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 3.1. CA files**

<code>cert_hash.0</code>	The trusted <i>CA Certificate</i> .
<code>cert_hash.signing_policy</code>	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.

WS Java-based components ignore the signing policy file and will honor all valid certificates issued by trusted CAs. [fixme - what about ws c-based components?]

### 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 [here](https://www.tacar.org/certs.html)<sup>1</sup>.

## 2. Configuring Globus to Create Appropriate Certificate Requests

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

---

<sup>1</sup> <https://www.tacar.org/certs.html>

**Table 3.2. Certificate request configuration files**

<code>globus-user-ssl.conf</code>	Defines the distinguished name to use for a user's certificate request. The format is described <a href="#">here</a> <sup>2</sup> .
<code>globus-host-ssl.conf</code>	Defines the distinguished name for a host (or service) certificate request. The format is described <a href="#">here</a> <sup>3</sup> .
<code>grid-security.conf</code>	A base configuration file that contains the name and email address for the CA.
<code>directions</code>	An optional file that may contain directions on using the CA.

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

You can specify a default CA for certificate requests (i.e., a CA that will be used if **grid-cert-request** is invoked without the `-ca` flag) by making the following symbolic links (where `GRID_SECURITY` is the *grid security directory* and `TRUSTED_CA` is the *trusted CAs directory*):

```
ln -s TRUSTED_CA/globus-user-ssl.conf.cert_hash \
    GRID_SECURITY/globus-user-ssl.conf
ln -s TRUSTED_CA/globus-host-ssl.conf.cert_hash \
    GRID_SECURITY/globus-host-ssl.conf
ln -s TRUSTED_CA/grid_security.conf.cert_hash \
    GRID_SECURITY/grid_security.conf
```

And optionally, if the CA-specific `directions` file exists:

<sup>2</sup> [http://www.openssl.org/docs/apps/req.html#CONFIGURATION\\_FILE\\_FORMAT](http://www.openssl.org/docs/apps/req.html#CONFIGURATION_FILE_FORMAT)

<sup>3</sup> [http://www.openssl.org/docs/apps/req.html#CONFIGURATION\\_FILE\\_FORMAT](http://www.openssl.org/docs/apps/req.html#CONFIGURATION_FILE_FORMAT)

```
ln -s TRUSTED_CA/directions.cert_hash \
    GRID_SECURITY/directions
```

This can also be accomplished by invoking the **grid-default-ca** 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 3.3. Certificate request files**

<code>GRID_SECURITY/service_name/service_namecert.pem</code>	An empty file. When you receive your actual service certificate from your CA, you should place it in this file.
<code>GRID_SECURITY/service_name/service_namecert_request.pem</code>	The certificate request, which you should send to your CA.
<code>GRID_SECURITY/service_name/service_namekey.pem</code>	The <i>private key</i> associated with your certificate request, encrypted with the pass phrase that you entered when prompted by <b>grid-cert-request</b> .

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

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

## 4. Specifying Identity Mapping Information (gridmap file)

Several Globus services map distinguished names (found in certificates) to local identities (e.g., unix logins). These mappings are maintained in the *gridmap* file.

### 4.1. Gridmap location

The location of the *gridmap* file is determined as follows:

1. GRIDMAP environment variable
2. `/etc/grid-security/grid-mapfile`
3. `$HOME/.gridmap`

### 4.2. 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.

### 4.3. Managing gridmap files

Several tools exist to manage grid map files. These commands recognize several useful options, including a `-help` option, which lists detailed usage information.

#### 4.3.1. 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
```

#### 4.3.2. 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
```

### 4.3.3. Checking consistency of a gridmap file

To check the consistency of the gridmap file, run

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

## 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:
  - 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 4. 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 `$GLOBUS_LOCATION/etc/grid-security/hostcert.pem` and `$GLOBUS_LOCATION/etc/grid-security/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*:

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 `usercert.pem` and `userkey.pem` exist in the user's `.globus` directory, those files are used.
3. 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 this 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 (Generic Authorization and Access control) 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.

# Appendix A. Errors

DRAFT

**Table A.1. Credential Errors**

<b>Error Code</b>	<b>Definition</b>	<b>Possible Solutions</b>
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> ).  <b>Important:</b> 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.  <b>Important:</b> 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 <a href="#">Installing GT 4.2.0</a> 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 <a href="#">Installing GT 4.2.0</a> 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).

**Table A.2. Gridmap Errors**

<b>Error Code</b>	<b>Definition</b>	<b>Possible Solutions</b>
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 <a href="#">grid-mapfile-check-consistency</a> 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 <a href="#">grid-mapfile-add-entry</a> to add the relevant entry.

DRAFT

# Glossary

## C

Certificate Authority ( CA )	An entity that issues certificates. [fixme - flesh out]
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 <code>/etc/grid-security/certificates/&lt;hash&gt;.0</code> , where <code>&lt;hash&gt;</code> 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 <code>/etc/grid-security/certificates/&lt;hash&gt;.signing_policy</code> , where <code>&lt;hash&gt;</code> 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 <code>/etc/grid-security/gsi-gaa.conf</code> .
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 <code>/etc/grid-security/grid-mapfile</code> . For more information see the Gridmap section <a href="#">here</a> .
grid security directory	The directory containing GSI configuration files such as the GSI authorization callout configuration and GAA configuration files. Typically this directory is <code>/etc/grid-security</code> . For more information see <a href="#">this</a> .
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 <code>/etc/grid-security/gsi-authz.conf</code> .

## H

host certificate	An EEC belonging to a host. When using GSI this certificate is typically stored in <code>/etc/grid-security/hostcert.pem</code> . For more information on possible host certificate locations see the <a href="#">GSI C Developer's Guide</a> .
host credentials	The combination of a host certificate and its corresponding private key.

## 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>/<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>.

**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>/<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.

## T

**trusted CAs directory** The directory containing the CA certificates and signing policy files of the CAs trusted by GSI. Typically this directory is `/etc/grid-security/certificates`. For more information see [this](#).

## 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.