GT 5.0.4 GSI C Public Interfaces
GT 5.0.4 GSI C Public Interfaces
# Table of Contents

1. APIs .............................................................................................................................................. 1
2. Protocol Specifications ...................................................................................................................... 3
   1. GSI Message Specification ......................................................................................................... 3
I. GSI Commands ................................................................................................................................ 4
   globus-update-certificate-dir .......................................................................................................... 5
   grid-cert-diagnostics ..................................................................................................................... 6
   grid-cert-info .............................................................................................................................. 8
   grid-cert-request ........................................................................................................................ 10
   grid-default-ca ........................................................................................................................... 14
   grid-change-pass-phrase ................................................................................................................ 16
   grid-proxy-init ........................................................................................................................... 17
   grid-proxy-destroy ..................................................................................................................... 20
   grid-proxy-info .......................................................................................................................... 21
   grid-mapfile-add-entry ................................................................................................................ 23
   grid-mapfile-check-consistency .................................................................................................... 25
   grid-mapfile-delete-entry ............................................................................................................. 27
3. Configuring Certificates ................................................................................................................... 29
   1. Configuring Globus to Trust a Particular Certificate Authority ......................................................... 29
   2. Configuring Globus to Create Appropriate Certificate Requests ....................................................... 30
   3. Requesting Service Certificates .................................................................................................. 32
   4. Configuring Credential Mappings .............................................................................................. 32
   5. GSI File Permissions Requirements ........................................................................................... 34
4. Environment variable interface .......................................................................................................... 36
   1. Environmental Variables for GSI C ............................................................................................ 36
A. Errors .......................................................................................................................................... 40
Glossary ........................................................................................................................................... 43
### List of Tables

3.1. CA files ..................................................................................................................................... 29  
3.2. Certificate request configuration files ......................................................................................... 30  
3.3. Certificate request files .................................................................................................................. 32  
3.4. Gridmap File Location Algorithm .................................................................................................. 33  
3.5. Authorization Configuration File Locations ..................................................................................... 34  
3.6. Authorization Configuration File Locations ..................................................................................... 34  
A.1. Credential Errors ........................................................................................................................... 41  
A.2. Gridmap Errors ............................................................................................................................. 42
Chapter 1. APIs

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

- [gaa_core](http://www.globus.org/api/c-globus-4.0/gaa_core/html/index.html#_top)
- [gaa_gss_generic](http://www.globus.org/api/c-globus-4.0/gaa_gss_generic/html/index.html#_top)
- [gaa_plugin](http://www.globus.org/api/c-globus-4.0/gaa_plugin/html/index.html#_top)
- [globus_authz](http://www.globus.org/api/c-globus-4.0/globus_authz/html/index.html#_top)
- [globus_authz_callout_error](http://www.globus.org/api/c-globus-4.0/globus_authz_callout_error/html/index.html#_top)
- [globus_gridmap_callout_error](http://www.globus.org/api/c-globus-4.0/globus_gridmap_callout_error/html/index.html#_top)
- [globus_gsi_callback](http://www.globus.org/api/c-globus-4.0/globus_gsi_callback/html/index.html#_top)
- [globus_gsi_cert_utils](http://www.globus.org/api/c-globus-4.0/globus_gsi_cert_utils/html/index.html#_top)
- [globus_gsi_credential](http://www.globus.org/api/c-globus-4.0/globus_gsi_credential/html/index.html#_top)
- [globus_gsi_openssl_error](http://www.globus.org/api/c-globus-4.0/globus_gsi_openssl_error/html/index.html#_top)
- [globus_gsi_proxy_core](http://www.globus.org/api/c-globus-4.0/globus_gsi_proxy_core/html/index.html#_top)
- [globus_gsi_proxy_ssl](http://www.globus.org/api/c-globus-4.0/globus_gsi_proxy_ssl/html/index.html#_top)
- [globus_gsi_sysconfig](http://www.globus.org/api/c-globus-4.0/globus_gsi_sysconfig/html/index.html#_top)
- [globus_gss_assist](http://www.globus.org/api/c-globus-4.0/globus_gss_assist/html/index.html#_top)
APIs

- `globus_gssapi_gsi`[^29] [no frames][^30]
- `globus_openssl_module`[^31] [no frames][^32]
- `gssapi_error`[^33] [no frames][^34]

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

[^29]: http://www.globus.org/api/c-globus-4.0/globus_gssapi_gsi/html/index.html#_top
[^31]: http://www.globus.org/api/c-globus-4.0/globus_openssl_module/html/index.html#_top
[^33]: http://www.globus.org/api/c-globus-4.0/gssapi_error/html/index.html#_top
[^34]: 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\(^1\).

\(^1\)../GSI-message-specification-02.doc
GSI Commands
Name

globus-update-certificate-dir -- Update symlinks in the trusted CA directory

globus-update-certificate-dir [-help] [-d DIRECTORY]

Description

The **globus-update-certificate-dir** program creates symlinks between files (CA certificates, certificate revocation lists, signing policy, and certificate request configuration files) using the certificate hash the installed version of OpenSSL uses. OpenSSL 1.0.0 uses a different name hashing algorithm than previous versions, so CA distributions created with older versions of OpenSSL might not be able to locate trusted CAs and related files. Running **globus-update-certificate-dir** against a trusted CA directory will add symlinks to the files to the hash if needed.

The full set of command-line options to **globus-update-certificate-dir** consists of:

- **-help** Display a help message to standard output and exit
- **-d DIRECTORY** Create links in the trusted CA directory **DIRECTORY** instead of using the default search path.

Environment

If the following variables affect the execution of **globus-update-certificate-dir**

**X509_CERT_DIR** Default trusted certificate directory.

**HOME** Path to the current user's home directory.

**GLOBUS_LOCATION** Path to the Globus installation.
Name

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


Description

The grid-cert-diagnostics program 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 GSIC.

By default, grid-cert-diagnostics prints out information regarding the environment and trusted certificate directory. If the -p command-line option is used, then additional information about the current user's default certificate and key will be printed.

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

- h, -help
  Display a help message and exit.

- p
  Display information about the personal certificate and key that is the current user's default credential.

- n
  Check time synchronization with the ntpdate command.

- c CERTIFICATE, -c -
  Check the validity of the certificate in the file named by CERTIFICATE or standard input if the parameter to -c is -.

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:
    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"
Reading certificate... ok
Reading 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
Private key modulus: D294849E37F048C3B5ACEEF2CCDF97D88B679C361E29D5CB5
219C3E948F3E530CFC609489759E1D751F0A1FF05151A614276A0F4C11A57D927165B8
FA64E3140155DE448D45C182F4657DA13EDA288423F5B9D169DDF3822ED81EB2E6403
CE3CB4CCF96B65284D92592B1673A18354DA241B9AFD7F494ED54F63A93E15DCAE2
Public key modulus : C002C7B329B13BFA87BAF214EACE3DC3D490165AEB791790
600708C544175D9193C9BAC5AE0D3B7CB49BB6AE6D29B7E63FAC751E9A6D1CEA98022
6F1B63002902D6623A319E4682E7BFB0968DCE962CF218AAD95FAAD6A0BA5C42AA9AF
7FDD32B37C62B2F0EB311310AA55FFBF9EAFDF5B995C7D8EAD8D5D81F3531E0AE5
Certificate and private key don't match
Name

grid-cert-info -- Display information about a certificate

grid-cert-info [-file CERTIFICATE-FILE] [-rfc2253] [-all]
[-subject] [-s]
[-issuer] [-i]
[-issuerhash] [-ih]
[-startdate] [-sd]
[-enddate] [-ed]

Description

The grid-cert-info program displays information contained within a certificate file. By default it shows a text representation of the entire certificate. Specific facts about the certificate can be shown instead by using command-line options. If any of those options are used, then the default display is suppressed. This can be added to the output by using the -all command-line option.

If multiple display options are included on the command-line, the facts related to those will be displayed on separate lines in the order that they occur. If an option is specified multiple times, that fact will be displayed multiple times.

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

- help, -usage
  Display the command-line options to grid-cert-info and exit.

- version, -versions
  Display the version number of the grid-cert-info command. The second form includes more details.

- file CERTIFICATE-FILE
  Display information about the first certificate contained in the file named by CERTIFICATE-FILE instead of the default user certificate.

- rfc2253
  Display X.509 distinguished names using the string representation defined in RFC 2253 instead of the default OpenSSL oneline format.

- all
  Display the text representation of the entire certificate in addition to any other facts requested by command-line options. This is the default if no fact-specific command-line options are used.

- subject, -s
  Display the subject name of the X.509 certificate.

- issuer, -i
  Display the issuer name of the X.509 certificate.

- issuerhash, -ih
  Display the default hash of the issuer name of the X.509 certificate. This can be used to locate which CA certificate in the trusted certificate directory issued the certificate being inspected.

-startdate, -sd
  Display a string representation of the date and time when the certificate is valid from. This is displayed in the format used by the OpenSSL x509 command.

-enddate, -dd
  Display a string representation of the date and time when the certificate is valid until. This is displayed in the format used by the OpenSSL x509 command.
Examples

Display the validity times for the default certificate

```
% grid-cert-info -sd -ed
Aug 31 12:33:47 2009 GMT
Aug 31 12:33:47 2010 GMT
```

Display the same information about a different certificate specified on the command-line

```
% grid-cert-info -sd -ed -f /etc/grid-security/hostcert.pem
Jan 21 12:24:48 2003 GMT
Jul 15 11:30:57 2020 GMT
```

Display the subject of a certificate in both the default and the RFC 2253 forms.

```
% grid-cert-info -subject
/DC=org/DC=example/DC=grid/CN=Joe User
% grid-cert-info -subject -rfc2253
CN=Joe User,DC=grid,DC=example,DC=org
```

Environment Variables

The following environment variables affect the execution of `grid-cert-info`:

- `X509_USER_CERT` Path to the default certificate file to inspect.
Name

grid-cert-request -- Generate a X.509 certificate request and corresponding private key

grid-cert-request [-help] [-h] [-?] [-usage]
[-version] [-versions]
grid-cert-request [-cn NAME] [-commonname NAME]
[-dir DIRECTORY] [-prefix PREFIX]
[-nopw] [-nodes] [-nopassphrase]
[-ca [HASH]] [-verbose] [-interactive] [-int] [-force]
grid-cert-request -host FQDN [-service SERVICE] [-dns FQDN...] [-ip IP-ADDRESS...]
[-dir DIRECTORY] [-prefix PREFIX]
[-ca [HASH]] [-verbose] [-interactive] [-int] [-force]

Description

The grid-cert-request program generates an X.509 Certificate Request and corresponding private key for the specified name, host, or service. It is intended to be used with a CA implemented using the globus_simple_ca package.

The default behavior of grid-cert-request is to generate a certificate request and private key for the user running the command. The subject name is derived from the gecos information in the local system's password database, unless the -commonname, -cn, or -host command-line options are used.

By default, grid-cert-request writes user certificate requests and keys to the $HOME/.globus directory, and host and service certificate requests and keys to /etc/grid-security. This can be overridden by using the -dir command-line option.

The full set of command-line options to grid-cert-request are:

-help, -h, -?, -usage Display the command-line options to grid-cert-request and exit.

-version, -versions Display the version number of the grid-cert-request command. The second form includes more details.

-cn NAME, -commonname NAME Create a certificate request with the common name component of the subject set to NAME. This is used to create user identity certificates.

-dir DIRECTORY Write the certificate request and key to files in the directory specified by DIRECTORY.

-prefix PREFIX Use the string PREFIX as the base name of the certificate, certificate_request, and key files instead of the default. For a user certificate request, this would mean creating files $HOME/.globus/PREFIXcert_request.pem, $HOME/.globus/PREFIXcert.pem, and $HOME/.globus/PREFIXkey.pem.

-ca CA-HASH Use the certificate request configuration for the CA with the name hash CA-HASH instead of the default CA chosen by running grid-default-ca.

-verbose Keep the output from the OpenSSL certificate request command visible after it completes, instead of clearing the screen.

-interactive, -int Prompt for each component of the subject name of the request, instead of generating the common name from other command-line options. Note that CAs may not sign certificates for subject names that don’t match their signing policies.
-force
Overwrite any existing certificate request and private key with a new one.

-nopw, -nodes, -no-passphrase
Create an unencrypted private key for the certificate instead of prompting for a passphrase. This is the default behavior for host or service certificates, but not recommended for user certificates.

-host FQDN
Create a certificate request for use on a particular host. This option also causes the private key associated with the certificate request to be unencrypted. The FQDN argument to this option should be the fully qualified domain name of the host that will use this certificate. The subject name of the certificate will be derived from the FQDN and the service option if specified by the -service command-line option. If the host for the certificate has multiple names, then use either the -dns or -ip command-line options to add alternate names or addresses to the certificates.

-service SERVICE
Create a certificate request for a particular service on a host. The subject name of the certificate will be derived from the FQDN passed as the argument to the -host command-line option and the SERVICE string.

-dns FQDN,...
Create a certificate request containing a subjectAltName extension containing one or more host names. This is used when a certificate may be used by multiple virtual servers or if a host has different names when contacted within or outside a private network. Multiple DNS names can be included in the extension by separating them with a comma.

-ip IP-ADDRESS,...
Create a certificate request containing a subjectAltName extension containing the IP addresses named by the IP-ADDRESS strings. This is used when a certificate may be used by services listening on multiple networks. Multiple IP addresses can be included in the extension by separating them with a comma.

Examples

Create a user certificate request:

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

/O=org/OU=example/OU=grid/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 Example CA 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 Example CA at ca@grid.example.org

Create a host certificate for a host with two names.

```
% grid-cert-request -host grid.example.org -dns grid.example.org,grid-internal.example.org
```

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

```
/O=org/OU=example/OU=grid/CN=host/grid.example.org
```

The private key is stored in /etc/grid-security/hostkey.pem
The request is stored in /etc/grid-security/hostcert_request.pem

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

```
cat /etc/grid-security/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 Example CA at ca@grid.example.org

**Environment Variables**

The following environment variables affect the execution of `grid-cert-request`:

- **X509_CERT_DIR**  
  Path to the directory containing SSL configuration files for generating certificate requests.

- **GRID_SECURITY_DIR**  
  Path to the directory containing SSL configuration files for generating certificate requests. This value is used if X509_CERT_DIR is not set.

- **GLOBUS_LOCATION**  
  Path to the directory containing the Globus Toolkit. This is searched if neither the X509_CERT_DIR nor the GRID_SECURITY_DIR environment variables are set.

**Files**

- **$HOME/.globus/usercert_request.pem**  
  Default path to write a user certificate request.

- **$HOME/.globus/usercert.pem**  
  Default path to write a user certificate.

- **$HOME/.globus/userkey.pem**  
  Default path to write a user private key.
<table>
<thead>
<tr>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/etc/grid-security/host-cert_request.pem</td>
<td>Default path to write a host certificate request.</td>
</tr>
<tr>
<td>/etc/grid-security/host-cert.pem</td>
<td>Default path to write a host certificate.</td>
</tr>
<tr>
<td>/etc/grid-security/hostkey.pem</td>
<td>Default path to write a host private key.</td>
</tr>
<tr>
<td>TRUSTED-CERT-DIR/globus-user-ssl.conf, TRUSTED-CERT-DIR/globus-user-ssl.conf.CA-HASH</td>
<td>SSL configuration file for requesting a user certificate. The first form is the default location, the second form is used when the -ca command-line option is specified.</td>
</tr>
<tr>
<td>TRUSTED-CERT-DIR/globus-host-ssl.conf, TRUSTED-CERT-DIR/globus-host-ssl.conf.CA-HASH</td>
<td>SSL configuration file for requesting a host or service certificate. The first form is the default location, the second form is used when the -ca command-line option is specified.</td>
</tr>
</tbody>
</table>
**Name**

grid-default-ca -- Select default CA for certificate requests

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

**Description**

The `grid-default-ca` program sets the default certificate authority to use when the `grid-cert-request` script is run. The CA's certificate, configuration, and signing policy must be installed in the trusted certificate directory to be able to request certificates from that CA. Note that some CAs have different policies and use other tools to handle certificate requests. Please consult your CA's support staff if you unsure. The `grid-default-ca` is designed to work with CAs implemented using the globus_simple_ca package.

By default, the `grid-default-ca` program displays a list of installed CA certificates and the prompts the user for which one to set as the default. If invoked with the `-list` command-line option, `grid-default-ca` will print the list and not prompt nor set the default CA. If invoked with the `-ca` option, it will not list or prompt, but set the default CA to the one with the hash that matches the `CA-HASH` argument to that option. If `grid-default-ca` is used to set the default CA, the caller of this program must have write permissions to the trusted certificate directory.

The `grid-default-ca` program sets the CA in the one of the grid security directories. It looks in the directory named by the GRID_SECURITY_DIR environment, the X509_CERT_DIR, /etc/grid-security, and $GLOBUS_LOCATION/share/certificates.

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

- `-help, -h, -usage, -u`  Display the command-line options to `grid-default-ca` and exit.
- `-version, -versions`  Display the version number of the `grid-default-ca` command. The second form includes more details.
- `-dir CA-DIRECTORY`  Use the trusted certificate directory named by `CA-DIRECTORY` instead of the default.
- `-list`  Instead of changing the default CA, print out a list of all available CA certificates in the trusted certificate directory
- `-ca CA-HASH`  Set the default CA without displaying the list of choices or prompting. The CA file named by `CA-HASH` must exist.

**Examples**

List the contents of the trusted certificate directory that contain the string Example:

```
% grid-default-ca | grep Example
15) cd1186ff - /DC=org/DC=Example/DC=Grid/CN=Example CA
```

Choose that CA as the default:

```
% grid-default-ca -ca cd1186ff
```

setting the default CA to: /DC=org/DC=Example/DC=Grid/CN=Example CA
linking /etc/grid-security/certificates/grid-security.conf.cd1186ff to
/etc/grid-security/certificates/grid-security.conf

linking /etc/grid-security/certificates/grid-host-ssl.conf.cd1186ff to
/etc/grid-security/certificates/grid-host-ssl.conf

linking /etc/grid-security/certificates/grid-user-ssl.conf.cd1186ff to
/etc/grid-security/certificates/grid-user-ssl.conf

...done.

**Environment Variables**

The following environment variables affect the execution of `grid-default-ca`:

- GRID_SECURITY_DIRECTORY: Path to the default trusted certificate directory.
- X509_CERT_DIR: Path to the default trusted certificate directory.
- GLOBUS_LOCATION: Path to the Globus Toolkit installation directory.

**Bugs**

The `grid-default-ca` program displays CAs from all of the directories in its search list; however, `grid-cert-request` only uses the first which contains a grid security configuration.

The `grid-default-ca` program may display the same CA multiple times if it is located in multiple directories in its search path. However, it does not provide any information about which one would actually be used by the `grid-cert-request` command.

**See Also**

grid-cert-request(1)
Name

grid-change-pass-phrase -- Change the passphrase of a private key

grid-change-pass-phrase [-file PRIVATE-KEY]

Description

The grid-change-pass-phrase program changes the passphrase protecting a private key or PKCS12 bundle containing a private key and certificate. By default, grid-change-pass-phrase uses the X509_USER_KEY environment variable to locate the private key. If that is not set, then it looks for $HOME/.globus/userkey.pem and $HOME/.globus/usercred.p12 in succession. The path to a key can be specified by using the -file command-line option.

The full set of command-line options to grid-change-pass-phrase are:

- -help, -usage Display the command-line options to grid-change-pass-phrase and exit.
- -version, -versions Display the version number of the grid-change-pass-phrase command. The second form includes more details.
- -file PRIVATE-KEY Change the passphrase of the private key named by PRIVATE-KEY instead of the default.

Examples

Change the passphrase of the default private key:

% grid-change-pass-phrase

Enter pass phrase for /home/juser/.globus/userkey.pem:
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

Environment Variables

The following environment variables affect the execution of grid-change-pass-phrase:

X509_USER_KEY Path to the default private key file.
Name

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

grid-proxy-init [-help] [-usage] [-version]
grid-proxy-init [-debug] [-q] [-verify]
[-policy POLICYFILE]
([-draft] | [-old] | [-rfc])

Description

The grid-proxy-init program generates X.509 proxy certificates derived from the currently available certificate files. By default, this command generates a RFC 3820 Proxy Certificate with a 512 bit key valid for 12 hours in a file named /tmp/x509up_uUID. Command-line options and variables can modify the format, strength, lifetime, and location of the generated proxy certificate.

X.509 proxy certificates are short-lived certificates, signed usually by a user's identity certificate or another proxy certificate. The key associated with a proxy certificate is unencrypted, so applications can authenticate using a proxy identity without providing a passphrase.

Proxy certificates 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 (this is enforced by the GSI libraries), and should be deleted after they are no longer needed.

This version of grid-proxy-init supports three different proxy formats: the old proxy format used in early releases of the Globus Toolkit up to version 2.4.x, an IETF draft version of X.509 Proxy Certificate profile used in Globus Toolkit 3.0.x and 3.2.x, and the RFC 3820 profile used in Globus Toolkit Version 4.0.x and 4.2.x. By default, this version of grid-proxy-init creates an RFC 3820 compliant proxy. To create a proxy compatible with older versions of the Globus Toolkit, use the -old or -draft command-line options.

The full set of command-line options to grid-proxy-init are:

- help, -usage
  Display the command-line options to grid-proxy-init.

- version
  Display the version number of the grid-proxy-init command

- debug
  Display information about the path to the certificate and key used to generate the proxy certificate, the path to the trusted certificate directory, and verbose error messages

- q
  Suppress all output from grid-proxy-init except for passphrase prompts.

- verify
  Perform certificate chain validity checks on the generated proxy.

- valid HOURS:MINUTES, -hours HOURS
  Create a certificate that is valid for HOURS hours and MINUTES minutes. If not specified, the default of twelve hours and no minutes is used.

1 http://www.ietf.org/rfc/rfc3820.txt
-cert CERTFILE, -key KEYFILE
Create a proxy certificate signed by the certificate located in CERTFILE using the key located in KEYFILE. If not specified the default certificate and key will be used. This overrides the values of environment variables described below.

-certdir CERTDIR
Search CERTDIR for trusted certificates if verifying the proxy certificate. If not specified, the default trusted certificate search path is used. This overrides the value of the X509_CERT_DIR environment variable.

-out PROXYPATH
Write the generated proxy certificate file to PROXYPATH instead of the default path of /tmp/x509up_uUID.

-bits BITS
When creating the proxy certificate, use a BITS bit key instead of the default 512 bit keys.

-policy POLICYFILE
Add the certificate policy data described in POLICYFILE as the ProxyCertInfo X.509 extension to the generated proxy certificate.

-pl POLICY-OID, -policy-language POLICY-OID
Set the policy language identifier of the policy data specified by the -policy command-line option to the oid specified by the POLICY-OID string.

-path-length MAXIMUM
Set the maximum length of the chain of proxies that can be created by the generated proxy to MAXIMUM. If not set, the default of an unlimited proxy chain length is used.

-pwstdin
Read the private key's passphrase from stdin instead of reading input from the controlling tty. This is useful when scripting grid-proxy-init.

-limited
Create a limited proxy. Limited proxies are generally refused by process-creating services, but may be used to authorize with other services.

-independent
Create an independent proxy. An independent proxy is not treated as an impersonation proxy but as a separate identity for authorization purposes.

-draft
Create a IETF draft proxy instead of the default RFC 3280-compliant proxy. This type of proxy uses a non-standard proxy policy identifier. This might be useful for authenticating with older versions of the Globus Toolkit.

-old
Create a legacy proxy instead of the default RFC 3280-compliant proxy. This type of proxy uses a non-standard method of indicating that the certificate is a proxy and whether it is limited. This might be useful for authenticating with older versions of the Globus Toolkit.

-rfc
Create an RFC 3820-compliant proxy certificate. This is the default for this version of grid-proxy-init.

Examples
To create a proxy with the default lifetime and format, run the grid-proxy-init program with no arguments. For example:

% grid-proxy-init
Your identity: /DC=org/DC=example/CN=Joe User
Enter GRID pass phrase for this identity:
Creating proxy .................. Done
Your proxy is valid until: Thu Mar 18 03:48:05 2010
To create a stronger proxy that lasts for only 8 hours, use the `-hours` and `-bits` command-line options to `grid-proxy-init`. For example:

```
% grid-proxy-init -hours 8 -bits 1024
Your identity: /DC=org/DC=example/CN=Joe User
Enter GRID pass phrase for this identity: 
Creating proxy .................................. Done
Your proxy is valid until: Thu Mar 17 23:48:05 2010
```

## Environment Variables

The following environment variables affect the execution of `grid-proxy-init`:

- **X509_USER_CERT**: Path to the certificate to use as issuer of the new proxy.
- **X509_USER_KEY**: Path to the key to use to sign the new proxy.
- **X509_CERT_DIR**: Path to the directory containing trusted certificate certificates and signing policies.

## Files

The following files affect the execution of `grid-proxy-init`:

- `$HOME/.globus/user-cert.pem`: Default path to the certificate to use as issuer of the new proxy.
- `$HOME/.globus/userkey.pem`: Default path to the key to use to sign the new proxy.

## Compatibility

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).

## See Also

`grid-proxy-destroy(1), grid-proxy-info(1)`
Name

grid-proxy-destroy -- Destroy the default proxy certificate

grid-proxy-destroy [-help] [-usage] [-version]

Description

The grid-proxy-destroy program removes X.509 proxy files from the local filesystem. It overwrites the data in the files and removes the files from the filesystem. By default, it removes the current user's default proxy (either /tmp/x509up_uUID where UID is the current POSIX user id, or the file pointed to by the X509_USER_PROXY environment variable) unless a list of proxy file paths are included as part of the command line.

Use the -- command-line option to separate a list of proxy paths from command line options if the proxy file begins with the – character.

The full list of command-line options to grid-proxy-destroy are:

- help, -usage Display the command-line options to grid-proxy-destroy.
- version Display the version number of the grid-proxy-destroy command
- debug Display verbose error messages.
- dryrun Do not remove the proxy, but display the path of the files that would have been removed, or the directory where they would have been removed from if the –all command-line option is used.
- default Remove the default proxy in addition to the files included on the command-line. Only needed if other paths are included on the command-line.
- all Remove the default proxy and all delegated proxies in the temporary file directory.

Environment Variables

The following environment variables affect the execution of grid-proxy-destroy:

X509_USER_PROXY Path to the default user proxy.

See Also

grid-proxy-init(1), grid-proxy-info(1)
Name

grid-proxy-info -- Display information about a proxy certificate

grid-proxy-info [-help] [-usage] [-version]
grid-proxy-info [[-subject] [-s]]
[[-issuer] [-i]]
[[-exists] [-e]]
[[[-valid HOURS:MINUTES] | [-v HOURS:MINUTES]]
[[[hours HOURS] | [-h HOURS]]
[[[-bits BITS] | [-b BITS]]]

Description

The grid-proxy-info program extracts information from an X.509 proxy certificates, and optionally displays or returns an exit code based on that information.

The default mode of operation is to print the following facts about the current user’s default proxy: subject, issuer, identity, type, strength, path, and time left. If the command-line option -exists or -e is included in the command-line, nothing is printed unless one of the print options is specified. Instead, grid-proxy-info determines if a valid proxy exists and, if so, exits with the exit code 0; if a proxy does not exist or is not valid, grid-proxy-info exits with the exit code 1. Additional validity criteria can be added by using the -valid, -v, -hours, -h, -bits, or -b command-line options. If used, these options must occur after the -e or -exists command-line options. Those options are only valid if one of the -e or -exists command-line options is used.

The complete set of command-line options to grid-proxy-info are:

- -help, -usage Display the command-line options to grid-proxy-info.
- -version Display the version number of the grid-proxy-info command
- -debug Display verbose error messages.
- -file PROXYFILE, -f PROXYFILE Read the proxy located in the file PROXYFILE instead of using the default proxy.
- -subject, -s Display the proxy certificate’s subject distinguished name.
- -issuer, -i Display the proxy certificate issuer’s distinguished name.
- -identity Display the proxy certificate’s identity. For non-independent proxies, the identity is the subject of the certificate which issued the first proxy in the proxy chain.
- -type Display the type of proxy certificate. The type string includes the format (“legacy”, “draft”, or RFC 3280 compliant), identity type (“impersonation” or “independent”), and policy (“limited” or “full”). See grid-proxy-init(1) for information about how to create different types of proxies.
- -timeleft Display the number of seconds remaining until the proxy certificate expires.
- -strength Display the strength (in bits) of the key associated with the proxy certificate.
- -all Display the default information for the proxy when also using the -e or -exists command-line option.
grid-proxy-info

-`text` Display the proxy certificate contents to standard output, including policy information, issuer, public key, and modulus.

-`path` Display the path to the file containing the default proxy certificate.

-`rfc2253` Display distinguished names for the subject, issuer, and identity using the string representation described in RFC 2253, instead of the legacy format.

-`exists,-e` Perform an existence and validity check for the proxy. If a valid proxy exists and matches the criteria described by other command-line options (if any), exit with 0; otherwise, exit with 1. This option must be before other validity check predicate in the command-line options. If this option is specified, the output of the default facts about the proxy is disabled. Use the `-all` option to have the information displayed as well as the exit code set.

-`valid HOURS:MINUTES, -v HOURS:MINUTES, -hours HOURS,-h HOURS` Check that the proxy certificate is valid for at least `HOURS` hours and `MINUTES` minutes. If it is not, `grid-proxy-info` will exit with exit code 1.

-`bits BITS,-b BITS` Check that the proxy certificate key strength is at least `BITS` bits.

**Environment Variables**

The following environment variables affect the execution of `grid-proxy-info`:

`X509_USER_PROXY` Path to the default user proxy.

**See Also**

`grid-proxy-init(1), grid-proxy-destroy(1)`
Name

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

grid-mapfile-add-entry [-dn DISTINGUISHED-NAME] [-ln LOCAL-NAME...]
[[-d] | [-dryrun]]
[[-mapfile MAPFILE] | [-f MAPFILE]]

Description

The **grid-mapfile-add-entry** program adds a new mapping from an X.509 distinguished name to a local POSIX user name to a gridmap file. Gridmap files are used as a simple authorization method for services such as GRAM5 or GridFTP.

The **grid-mapfile-add-entry** program verifies that the **LOCAL-NAME** is a valid user name on the system on which it was run, and that the mapping between **DISTINGUISHED-NAME** and **LOCAL-NAME** does not already exist in the gridmap file.

By default, **grid-mapfile-add-entry** will modify the gridmap file named by the GRIDMAP environment variable if present, or the file /etc/grid-security/grid-mapfile if not. This can be changed by the use of the **-mapfile** or **-f** command-line options.

If the gridmap file does not exist, **grid-mapfile-add-entry** will create it. If it already exists, **grid-mapfile-add-entry** will save the current contents of the file to a new file with the string **.old** appended to the file name.

The full set of command-line options to **grid-mapfile-add-entry** are:

- **-help,** **-usage** Display the command-line options to **grid-mapfile-add-entry**.
- **-version,** **-versions** Display the version number of the **grid-mapfile-add-entry** command. The second form includes more details.
- **-dn DISTINGUISHED-NAME** The X.509 distinguished name to add a mapping for. The name should be in OpenSSL's oneline format.
- **-ln LOCAL-NAME...** The POSIX user name to map the distinguished name to. This name must be a valid username. Add multiple **LOCAL-NAME** strings after the **-ln** command-line option. If any of the local names are invalid, no changes will be made to the gridmap file. Note that if multiple occurrences of the **-ln** command-line option are present, only the the last one will be added.
- **-d,** **-dryrun** Verify local names and display diagnostics about what would be added to the gridmap file, but don't actually modify the file.
- **-mapfile MAPFILE,** **-f MAPFILE** Modify the gridmap file named by **MAPFILE** instead of the default.

Examples

Add a mapping between the current user's certificate to the current user id to a gridmap file in $HOME/.gridmap:

```
% grid-mapfile-add-entry -f $HOME/.gridmap -dn "`grid-cert-info -subject`" -ln "$id -un"
Modifying /home/juser/.gridmap ...
```
/home/juser/.gridmap does not exist... Attempting to create /home/juser/.gridmap

New entry:
"/DC=org/DC=example/DC=grid/CN=Joe User" juser
(1) entry added

Add a mapping between the a distinguished name and multiple local names:

% grid-mapfile-add-entry -dn "/DC=org/DC=example/DC=grid/CN=Joe User" juser" local1 local2

Modifying /home/juser/.gridmap ...

New entry:
"/DC=org/DC=example/DC=grid/CN=Joe User" local1,local2
(1) entry added

Environment Variables

The following environment variables affect the execution of grid-mapfile-add-entry:

GRIDMAP Path to the default gridmap to modify.

Files

The following files affect the execution of grid-mapfile-add-entry:

/etc/grid-security/grid-mapfile Path to the default gridmap to modify if GRIDMAP environment variable is not set.

See Also

grid-mapfile-check-consistency(8), grid-mapfile-delete-entry(8)
Name
grid-mapfile-check-consistency -- Add an entry to a grid map file

Usage:
grid-mapfile-check-consistency [-mapfile MAPFILE] [-f MAPFILE]

Description
The grid-mapfile-check-consistency program performs basic checks for validity of a gridmap file. These checks include checks for existence, duplication of entries, and valid local user names. If the gridmap file is valid, grid-mapfile-check-consistency exits with a zero exit code, otherwise it exits with a non-zero exit code. In either case, it displays information about its progress as it parses and validates the gridmap file.

By default, grid-mapfile-check-consistency will check the gridmap file named by the GRIDMAP environment variable if present. If that variable is not set, it will check the file $HOME/.gridmap for non-root users if present. If that doesn't exist or grid-mapfile-check-consistency is run as root, it will then check /etc/grid-security/grid-mapfile. This can be changed by the use of the -mapfile or -f command-line options.

The full set of command-line options to grid-mapfile-check-consistency are:
- -help, -h, -usage: Display the command-line options to grid-mapfile-check-consistency.
- -version: Display the version number of the grid-mapfile-check-consistency command.
- -mapfile MAPFILE, -f MAPFILE: Check the gridmap file named by MAPFILE instead of the default.

Examples
Check that the gridmap file in /etc/grid-security is valid:

% grid-mapfile-check-consistency -f /etc/grid-security/grid-mapfile
Checking /etc/grid-security/grid-mapfile
Verifying grid mapfile existence...OK
Checking for duplicate entries...OK
Checking for valid user names...OK

Check a gridmap file that has an invalid local user name:

% grid-mapfile-check-consistency -f /etc/grid-security/grid-mapfile
Checking /etc/grid-security/grid-mapfile
Verifying grid mapfile existence...OK
Checking for duplicate entries...OK
ERROR: baduser is not a valid local username
ERROR: Found 1 invalid username(s)

Environment Variables
The following environment variables affect the execution of grid-mapfile-check-consistency:

GRIDMAP Path to the default gridmap to check.
Files

The following files affect the execution of `grid-mapfile-check-consistency`:

<table>
<thead>
<tr>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$HOME/.gridmap</td>
<td>Path to the default gridmap to check if the GRIDMAP environment variable is not set for non-root users.</td>
</tr>
<tr>
<td>/etc/grid-security/gridmapfile</td>
<td>Path to the default gridmap to check if GRIDMAP environment variable is not set and the above file does not exist.</td>
</tr>
</tbody>
</table>

See Also

`grid-mapfile-add-entry(8)`, `grid-mapfile-delete-entry(8)`
Name

grid-mapfile-delete-entry -- Remove entries from a gridmap file

grid-mapfile-delete-entry { -dn DISTINGUISHED-NAME } [-ln LOCAL-NAME... ]
[ [-d] | [-dryrun] ]
[ [-mapfile MAPFILE] | [-f MAPFILE] ]

Description

The grid-mapfile-delete-entry program deletes mappings from a gridmap file. If both the -dn and -ln options are specified, grid-mapfile-delete-entry removes entries which meet both criteria (remove entries mapping DISTINGUISHED-NAME to LOCAL-NAME for each LOCAL-NAME specified). If only -dn or -ln is specified all entries for that DISTINGUISHED-NAME or LOCAL-NAME are removed.

By default, grid-mapfile-delete-entry will modify the gridmap file named by the GRIDMAP environment variable if present, or the file /etc/grid-security/grid-mapfile if not. This can be changed by the use of the -mapfile or -f command-line options.

Prior to modifying a gridmap file, grid-mapfile-delete-entry saves its current contents to a file with the string .old appended to the original file name.

The full set of command-line options to grid-mapfile-delete-entry are:

- help, -usage
  Display the command-line options to grid-mapfile-delete-entry.

- version, -versions
  Display the version number of the grid-mapfile-delete-entry command. The second form includes more details.

- dn DISTINGUISHED-NAME
  The X.509 distinguished name to remove from the gridmap file. If the -ln option is not specified, remove all entries for this name; otherwise, remove entries that match both this name and the local name. The name should be in OpenSSL's oneline format.

- ln LOCAL-NAME...
  The POSIX user name to remove from the gridmap file. Include multiple LOCAL-NAME strings after the -ln command-line option to remove multiple names from the gridmap. If the -dn option is not specified, remove all entries for these names; otherwise, remove entries that match the DISTINGUISHED-NAME and any of the LOCAL-NAME values.

- d, -dryrun
  Display diagnostics about what would be removed from the gridmap file, but don't actually modify the file.

- mapfile MAPFILE, -f MAPFILE
  Modify the gridmap file named by MAPFILE instead of the default.

Examples

Remove all mappings for a distinguished name:

% grid-mapfile-delete-entry " /DC=org/DC=example/DC=grid/CN=Joe User"
Modifying /etc/grid-security/grid-mapfile ...
Deleting entry: "/DC=org/DC=example/DC=grid/CN=Joe User" juser, juser2
(1) entry deleted

Remove the mapping between a distinguished name and a single local username:

% grid-mapfile-delete-entry "/DC=org/DC=example/DC=grid/CN=Joe User" -ln juser2
Modifying /etc/grid-security/grid-mapfile ...
Current entry: "/DC=org/DC=example/DC=grid/CN=Joe User" juser
(1) mapping removed: (juser2), (0) not present and ignored
(0) entries deleted

Environment Variables

The following environment variables affect the execution of grid-mapfile-delete-entry:

GRIDMAP Path to the default gridmap to modify.

Files

The following files affect the execution of grid-mapfile-delete-entry:

/etc/grid-security/grid-mapfile Path to the default gridmap to modify if GRIDMAP environment variable is not set.

See Also

grid-mapfile-add-entry(8), grid-mapfile-check-consistency(8)
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:

| 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 here.

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>
<thead>
<tr>
<th>Table 3.2. Certificate request configuration files</th>
</tr>
</thead>
<tbody>
<tr>
<td>globus-user-ssl.conf</td>
</tr>
<tr>
<td>globus-host-ssl.conf</td>
</tr>
<tr>
<td>grid-security.conf</td>
</tr>
<tr>
<td>directions</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 Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRID_SECURITY/service_name/service_namecert.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_namecert_request.pem</td>
<td>The certificate request, which you should send to your CA.</td>
</tr>
<tr>
<td>GRID_SECURITY/service_name/service_namekey.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 3.4. 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.

---

4.2. 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>
<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>
<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:

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

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/service.cert.pem` and `/etc/grid-security/service/service.key.pem` exist and contain a valid certificate and key, those files are used.
3. Otherwise, if the files `$GLOBUS_LOCATION/etc/grid-security/service/service.cert.pem` and `$GLOBUS_LOCATION/etc/grid-security/service/service.key.pem` exist and contain a valid certificate and key, those files are used.
4. Otherwise, if the files `service/service.cert.pem` and `service/service.key.pem` 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.

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:

- **Strictly backward-compatible with GT 2.0 name matching. X.509 subjectAltName values are ignored. Names with hyphens are treated as wildcarded as described in the security considerations documentation. Name matching will rely on canonical host name associated with connection IP addresses.** (GLOBUS_GSSAPI_NAME_COMPATIBILITY=STRICT_GT2)

- **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.** (GLOBUS_GSSAPI_NAME_COMPATIBILITY=STRICT_RFC2818)

---

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.
Appendix A. Errors
### Table A.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 5.0.4 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 5.0.4 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>
## Table A.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 <code>grid-mapfile-check-consistency</code> 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 <code>grid-mapfile-add-entry</code> to add the relevant entry.</td>
</tr>
</tbody>
</table>
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.
<table>
<thead>
<tr>
<th><strong>P</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>private key</td>
<td>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/&lt;service&gt;/key.pem (for service certificates). For more information on possible private key locations see this.</td>
</tr>
<tr>
<td>proxy credentials</td>
<td>The combination of a proxy certificate and its corresponding private key. GSI typically stores proxy credentials in /tmp/x509up_u&lt;uid&gt;, where &lt;uid&gt; is the user id of the proxy owner.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>S</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>service certificate</td>
<td>A EEC for a specific service (e.g. FTP or LDAP). When using GSI this certificate is typically stored in /etc/grid-security/&lt;service&gt;/&lt;service&gt;cert.pem. For more information on possible service certificate locations, see this.</td>
</tr>
<tr>
<td>service credentials</td>
<td>The combination of a service certificate and its corresponding private key.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>U</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>user certificate</td>
<td>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.</td>
</tr>
<tr>
<td>user credentials</td>
<td>The combination of a user certificate and its corresponding private key.</td>
</tr>
</tbody>
</table>