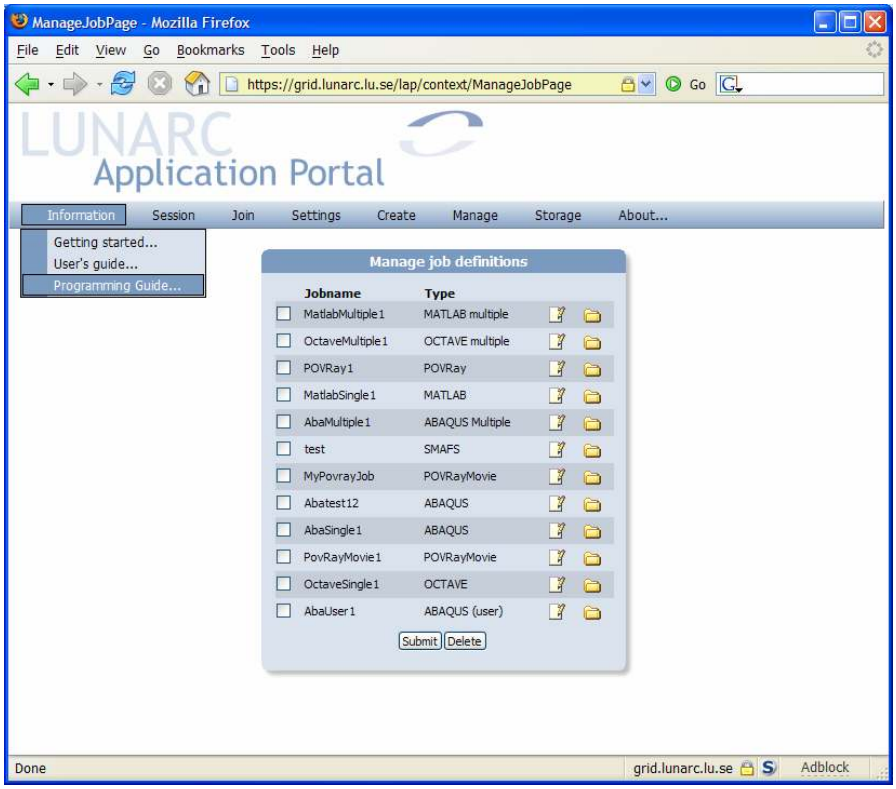
Lunarc Application Portal



Getting Started

1 Introduction

The Lunarc Application Portal is an effort to provide easy access grid resources for commonly available applications, such as MATLAB, Python, ABAQUS etc. The portal provides easy to use forms for each supported application where single and multiple jobs can created and submitted to the grid. Functions for controlling and monitoring jobs are also available.

As an additional service to the users a special client application has been developed, Grid Certificate Manager, which handles certificate request generation, grid proxy generation and certificate renewal. By using this application, the difficulties of using the grid portal should be reduced even further.

2 Getting access to the portal

To get access to the Lunarc Application Portal 3 steps are necessary. The steps (1) and (3) are not necessary to do every login.

❶ Getting a signed Grid Certificate

❷ Generating a proxy for logging into the portal

❸ Applying for membership in a VO

The grid certificate is the equivalent of a passport in the real world. In the same way as with a normal passport, your identity needs to be proven. On the Grid, this is done by sending your certificate request to a certificate authority that checks your identity and returns a signed certificate that can be used for authentication on grid resources. The signed certificate establishes your identity on the grid.

To be able to log in to the portal a special time limited token, proxy, is needed. This token is generated from the Grid Certificate. The proxy is securely uploaded using SSL to the portal to be able to act on the users behalf. When the user logs out of the portal the proxy is destroyed automatically.

The Grid Certificate does not automatically allow access to Grid resource. To get access to resources membership in a Virtual Organisation (VO) is also required. From within the portal request for membership in a VO can be made.

The steps above can be done either using from a graphical user interface, Grid Certificate Manager, or using the command line tools provided by the ARC software. The Grid Certificate Manager can be used both for Linux and for Windows users. The ARC client tools are only available on Linux.

2.1 Grid Certificate Manager

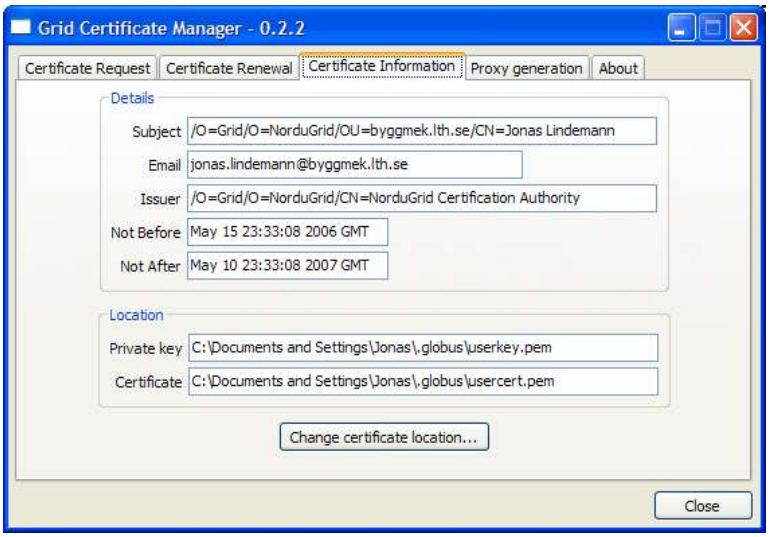
The Grid Certificate Manager is a standalone application providing a user interface for all the tasks involved managing grid certificates. The program is available for Microsoft Windows and most Linux distributions supporting Python 2.3 and wxWidgets.

2.1.1 Installing and starting the Grid Certificate Manager

The Grid Certificate manager has been packaged into a standard binary installation, which can be downloaded from http://www.lunarc.lu.se/Software/gridman. The installation is started by clicking on the downloaded `setup.exe` file. An installation guide is shown. The installation will also install OpenSSL on the computer as a separate installation. The Grid Certificate Manager installation will return after a completed OpenSSL installation.

The grid certificate manager is starting by selecting **Lunarc/Grid Certificate Manager** from the program menu in Windows.

2.1.2 Grid Certificate Manager Window Layout



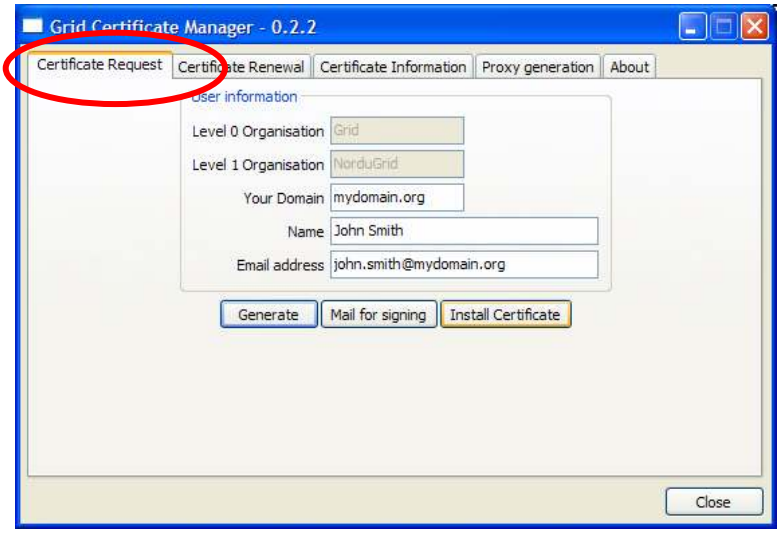
The Grid Certificate Window has four main tabs:

- **Certificate Request** – Handles generation of a certificate request and installation of a signed certificate.
- **Certificate Renewal** – Handles the renewal of an existing certificate and installation of a new certificate
- **Certificate Information** – Displays information on the installed certificate and corresponding private key.
- **Proxy Generation** – Handles creation of a grid proxy, used to when authenticating on the grid.

The usage of the described tabs are described in the following sections.

2.1.3 Generating a certificate request

The first step in getting a grid certificate is to generate a certificate request. This is done in the **Certificate Request** tab.



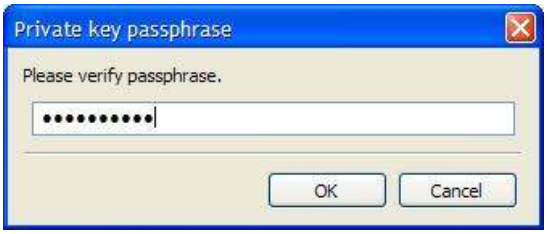
To complete the request 3 fields must be filled in:

- **Your Domain** – Your administrative domain (ex. mydomain.org).
- **Name** – Your real name (ex. John Smith)
- **Email adress** – Your email-adress. The domain after the @-sign should contain the same dmoain as in the **Your Domain** field.

To generate the request and private key, click **Generate**. A dialog is shown requesting a pass phrase for the private key.

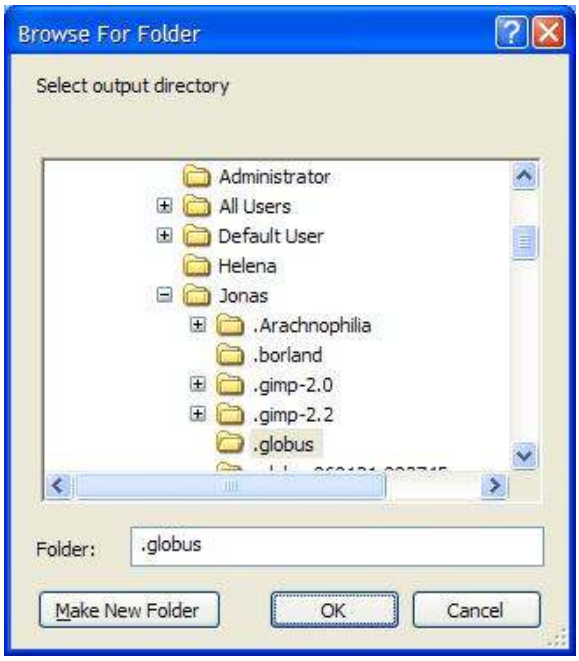
NOTE: the private key pass phrase is not related to any other password, and must be different from, e.g., your system login password. Memorize well the password, as it cannot be reset! Although you can change the password any time (see Section 4.2.7), if you forget the password, you will have to request a new certificate. [From the Nordugrid User's guide]

Enter the selected pass phrase and click **Ok** to continue. To verify that a correct pass phrase has been given a second dialog is shown asking for a verification.



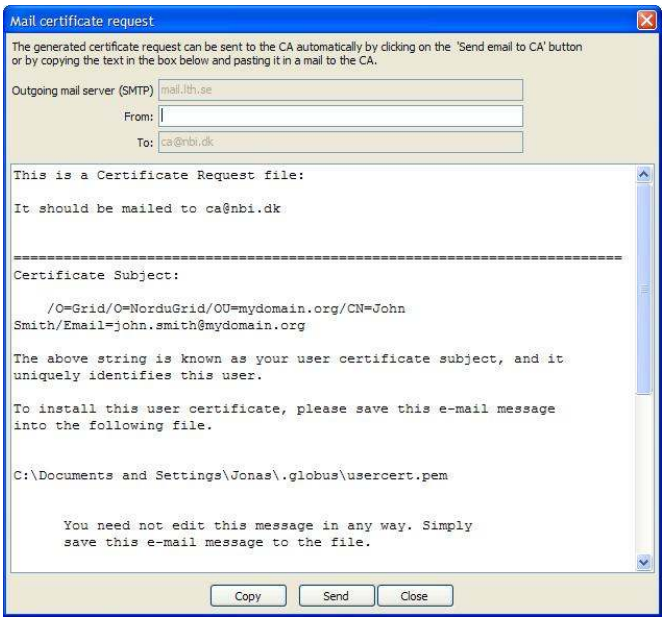
Click **OK** to continue. A new dialog is shown displaying a short summary of what is to be sent with the certificate request. Click **Yes** if the information is correct.

Next, a dialog is shown asking for where to store certificate information.



The default location is the ”Document and Settings\[User name]\.globus” folder on Windows. Click **OK** to accept the default location.

A certificate request (usercert_request.pem) has now been created together with a private key (userkey.pem). To get a signed certificate (usercert.pem) the certificate request must be mailed for signing. This is done by clicking on the **Mail for signing** button. This brings up a mail dialog containing the certificate request. Please enter your email address in the **From** field.



To mail the certificate request to the Certificate Authority click the **Send** button. To send the certificate request using a different mail client, click **Copy** to copy the request text to the clipboard and use **Ctrl+V** to paste into to the mail client.

A signed certificate should be mailed within a couple of days. Please see the next section on how to install this.

2.1.4 Installing signed certificate

In a couple of days after sending a certificate request, a signed certificate will be sent by mail. The Certificate Manager can be used to install this certificate as well. To install the received certificate select the following section in the mail:

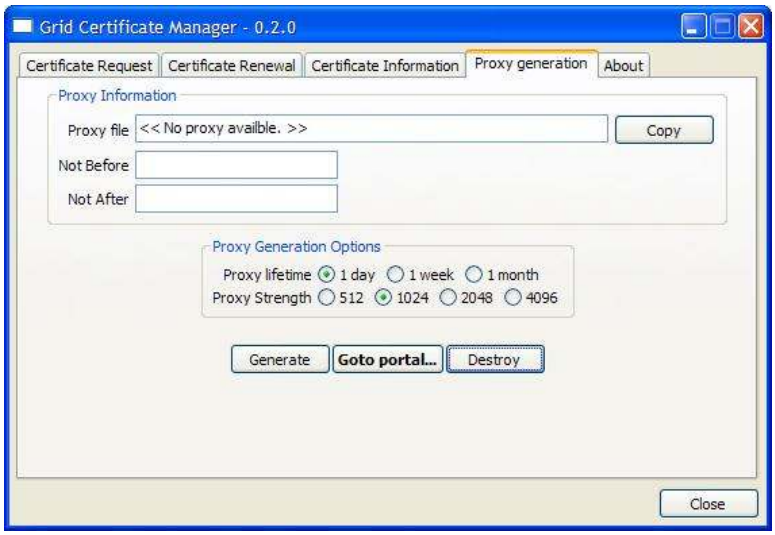
```
-----BEGIN CERTIFICATE-----
..
-----END CERTIFICATE-----
```

Copy the selection to the clipboard using either **Edit/Copy** from the menu or **Ctrl-C** from the keyboard. In the **Certificate request** tab in the Grid Certificate Manager window, click **Install certificate**. An empty window is shown with a large text box. Click **Paste** or **Ctrl-V** to paste the selected certificate contents in the text box. To install the certificate click **Install**.

AVOID STORING YOUR PRIVATE KEY ON A PUBLIC FACILITY, SUCH AS A SHARED ACCESS COMPUTER, KEEP IT ON YOUR PRIVATE COMPUTER INSTEAD. COMPROMISED KEYS ARE REVOKED BY THE AUTHORITY.

2.1.5 Generating a Grid proxy

Generation of a grid proxy is done from the **Proxy generation** tab.



To generate a grid proxy, press the **Generate** button. This will bring up a dialog box asking for the passphrase for the private key.

Enter the passphrase and click **OK**. The default proxy length is set to 1 day and with cipher strength of 1024 bits. This can be changed in the **Proxy Generation Options** radio boxes.

2.1.6 Logging in to the Lunarc Application Portal

Loggin in to the Application Portal is done by transferring the proxy file to the portal. To open a browser with the start page of the Portal click **Goto portal...** in the **Proxy generation** tab. To log in, select the **Log in** from the **Session** menu. This will bring up a login form.

Select the newly generated proxy-file using the **Browse...** button and press the **Login** button. As noted before the default location of the proxy-file is ”Document and Settings\[User name]\.globus”. The name of the file is of the format

“x509_up[Username]”.

To make it easier to select the proxy file, a special **Copy** button is located on the **Proxy generation** tab, which copies the location of the proxy-file to the clipboard. The contents of the clipboard can then directly be pasted into the login-form. The preferred login method is then as follows.

1. Generate the proxy.
2. Click **Copy** to transfer the proxy-file location to the clipboard
3. Clilck **Go to portal...** to open a browser with the portal start page.

2.2 ARC client tools

The ARC command line tool can also be used to get access to the Lunarc Application portal. Please see chapters 4, 5 and 6 of the Nordugrid User's Guide for extensive information on this topic.

2.2.1 Generating a grid proxy

A proxy file is generated using the following commands:

```
[user@system user]$ grid-proxy-init
Your identity: /O=Grid/O=NorduGrid/OU=mydomain.org/CN=John Smith
Enter GRID pass phrase for this identity:
Creating proxy ..................................... Done
Your proxy is valid until: Mon Feb 13 11:58:07 2006
```

This will generate a proxy file located /tmp. The format of the file is “x509_up[uid number]”

2.2.2 Logging in to the Lunarc Application Portal

Loggin in to the Application Portal is done by transferring the proxy file to the portal. Open the portal start page. To log in, select the **Log in** from the **Session** menu. This will bring up a login form.

Select the newly generated proxy-file using the **Browse** button and press the **Login** button. As noted before the default location of the proxy-file is ”Document and Settings\[User name]\.globus”. The name of the file is of the format “x509_up[Username]”.