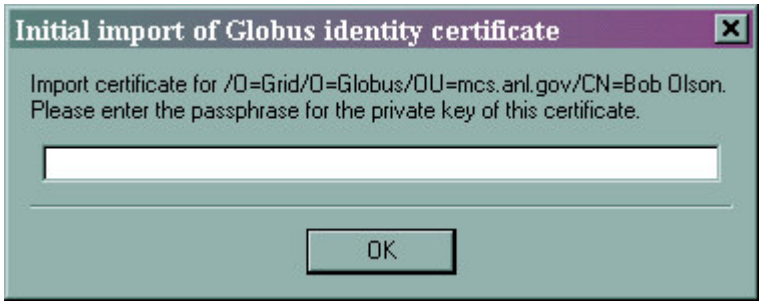
# Using the Certificate Manager in AG 2.1

The AG2.1 certificate manager keeps track of your identity certificates (used to prove to others that you are who you say you are) and your trusted CA certificates (used to determine which people you will trust).

If you have a working Globus environment, either on a Linux system or on a Windows system, that has had your identity certificate copied to it, the certificate manager should import this environment the first time you run the AG software. You will be prompted for the private key to your identity certificate so that it can be properly imported:




After the environment is initialized, the AG software will look for a valid Globus proxy certificate (this is a version of your identity certificate that is used in communicating with the AG venue server and with other clients). If one does not exist, a window will appear that asks you for the passphrase for your identity certificate. Enter the passphrase, click OK, and you should be up and running.

If you do not have an identity certificate, you will need to obtain one. You will need to determine from which Certificate Authority you wish to request a certificate.

For those in the DOE research community, the DOE Science Grid offers

certificate service. You can find this at

http://doesciencegrid.org/

If you are a member of the NCSA user community, you can request a

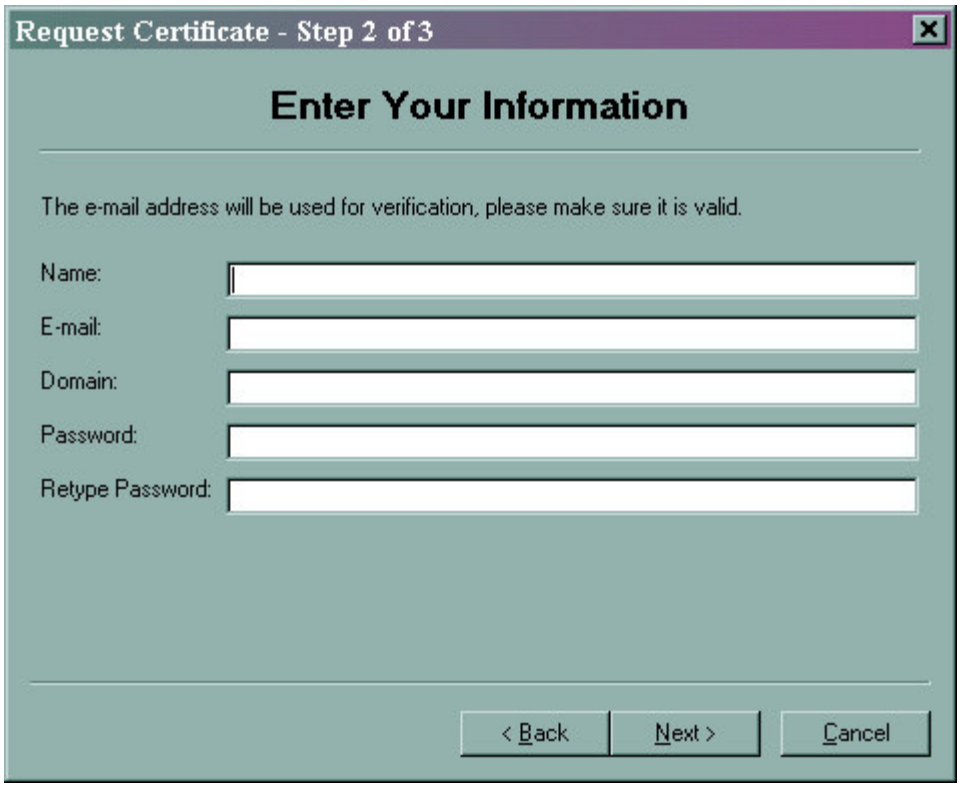
certificate from the NCSA CA at

http://www.ncsa.uiuc.edu/UserInfo/Grid/Security/GetUserCert.html

If you do not have another source for an identity certificate, you may request a certificate from the ANL Access Grid Developers' CA. You can do this using the certificate request tool that is part of the AG Venues Client.

If an identity certificate is not found when the AG Venue Client starts, it will invoke the certificate request tool. The following dialog will appear:

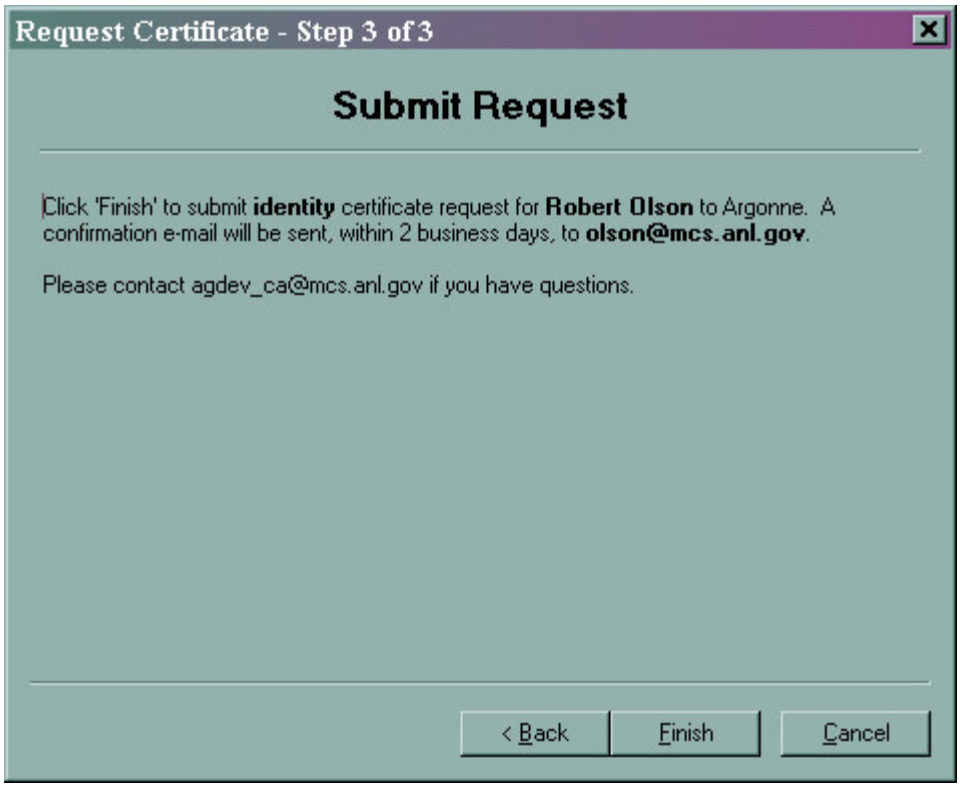

Clicking *Next* will bring you to this dialog:




Enter your name, a valid email address, and a domain name that represents the institution you are affiliated with. The dialog will default this value to the host part of your email address.

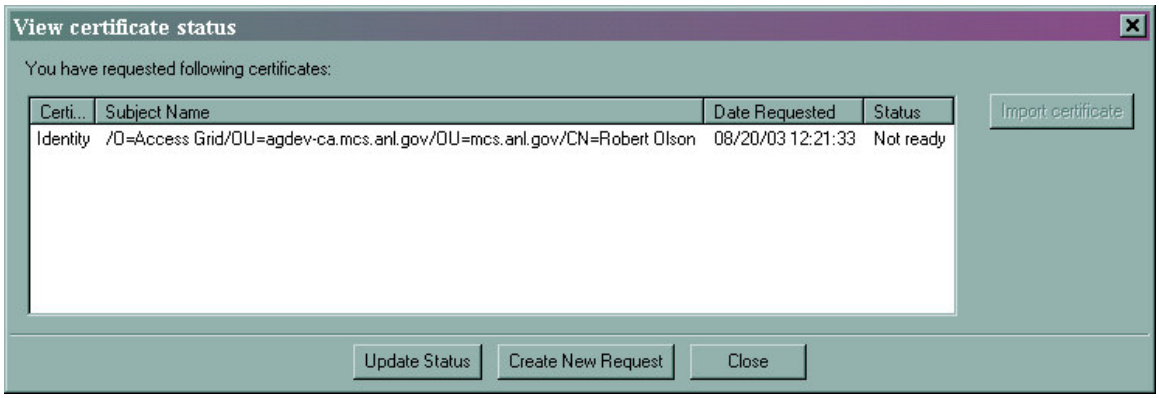
Then enter a password. This will be used to protect the private key for your certificate as it is stored on disk.

Pressing *Next* will bring you to this confirmation screen:



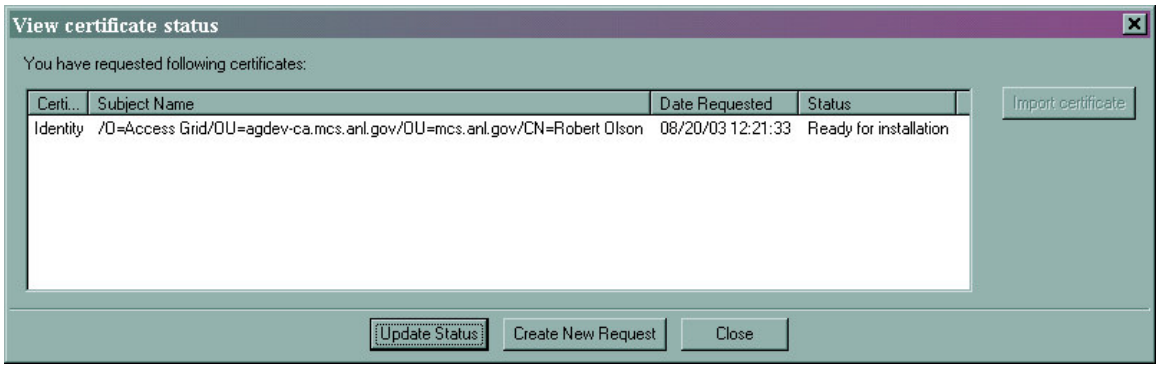

Upon pressing *Finish*, your certificate request will be submitted over the network to the request server at Argonne National Laboratory and the administrators notified via email.

The next time you start your venue client, you will be presented with a window like this:

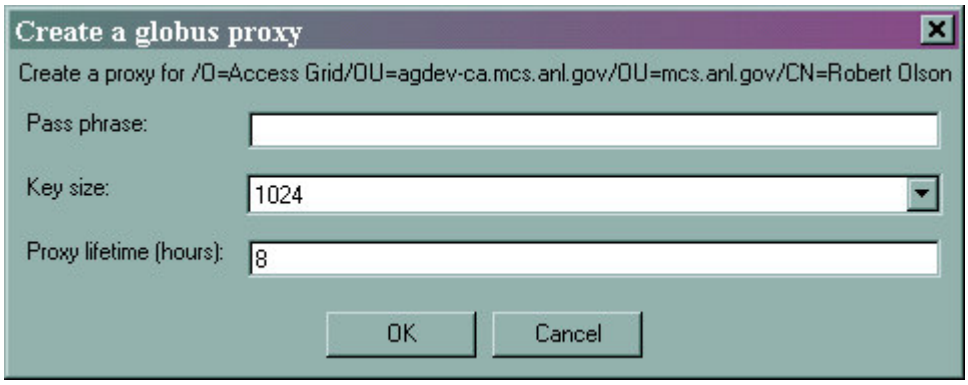



If the status column says “Not ready”, the certificate has not yet been signed. You can update the status by pressing the *Update Status* button.

When the certificate has been signed, the status window will look like this:



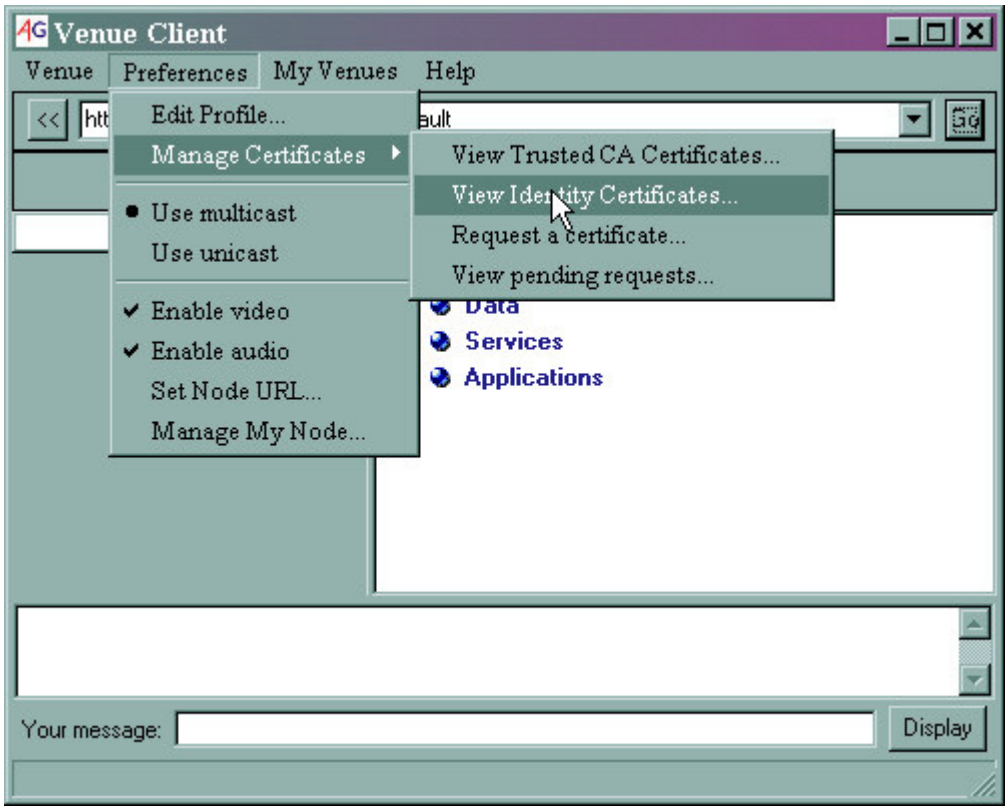

Click on the certificate name in the dialog, and press *Import Certificate.* If all goes well, you will be prompted to create a Globus proxy for the new certificate:



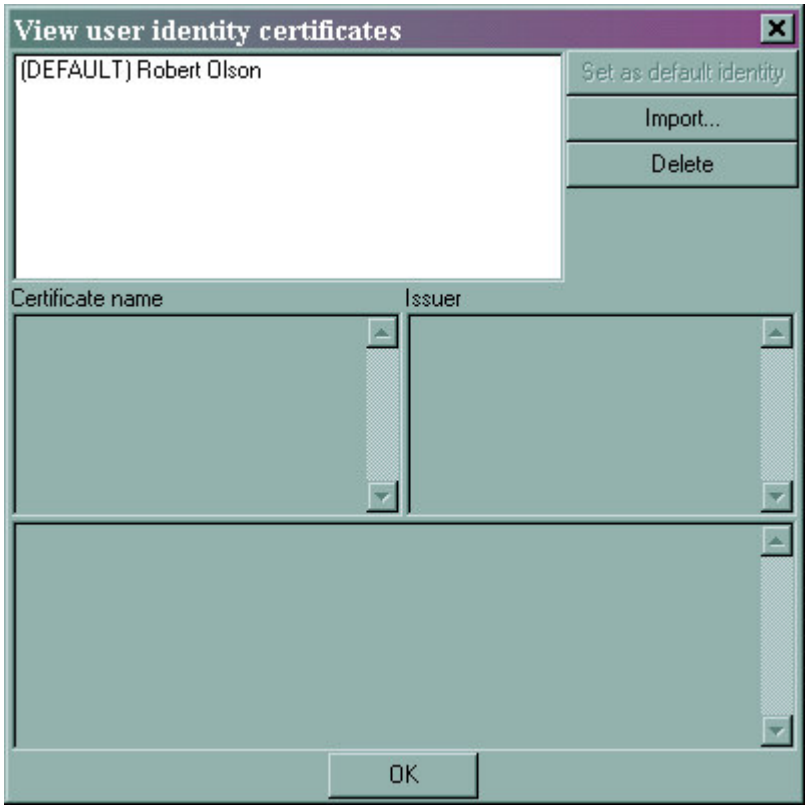

and then the following dialog will appear:


## Importing Identity Certificates

If you have an existing certificate, you can import it into the certificate manager using the GUI:




The *View Identity Certificates* menu brings up the certificate browser:



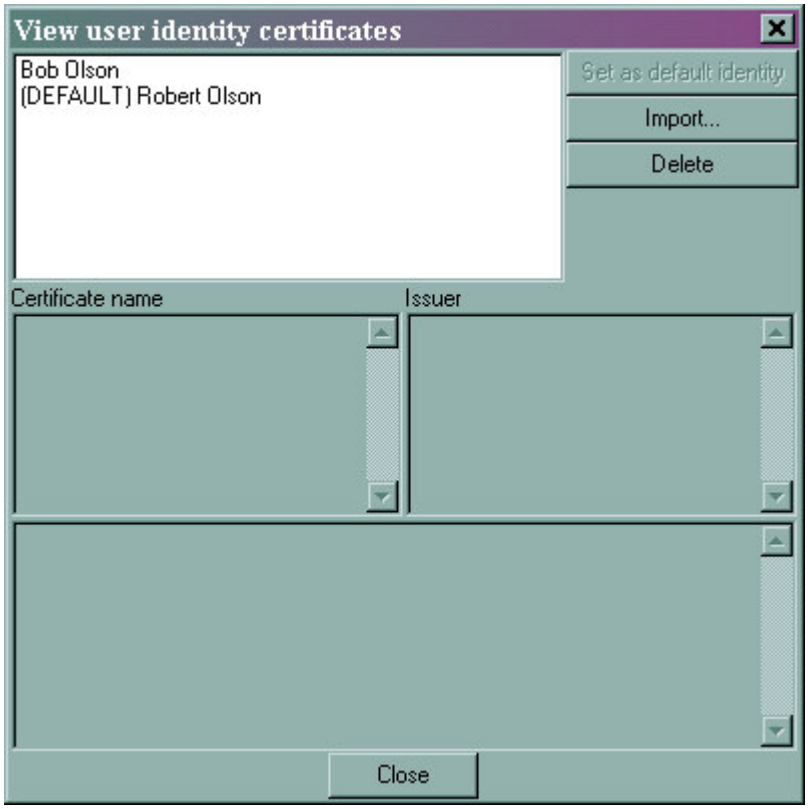
Press *Import* to import an existing certificate. A standard file browser will appear. Browse to your identity certificate file, and press *Open.* The certificate file must be in PEM format; that is, it will look something like the following:

```
-----BEGIN CERTIFICATE-----
MIICHTCCAYagAwIBAgICM64wDQYJKoZIhvcNAQEEBQAwRzELMAkGA1UEBhMCVVMx
DzANBgNVBAoTBkdsb2J1czEnMCUGA1UEAxMeR2xvYnVzIENlcnRpZmljYXRpb24g
-----END CERTIFICATE-----
```

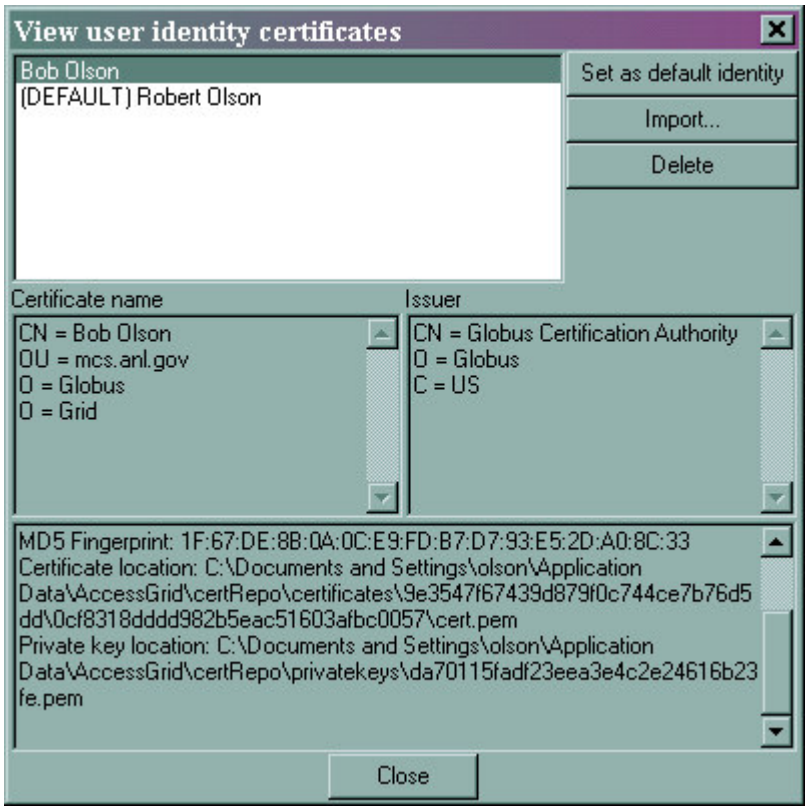
If the certificate file does not also contain a private key, a new file browser will open for you to browse to the location of the private key. Find the private key file, also a PEM-formatted file, and press *Open*.

A dialog will open prompting you to enter the passphrase for the private key:


Enter it, and press *OK*. If the import is successful, the new identity will appear in the browser window:



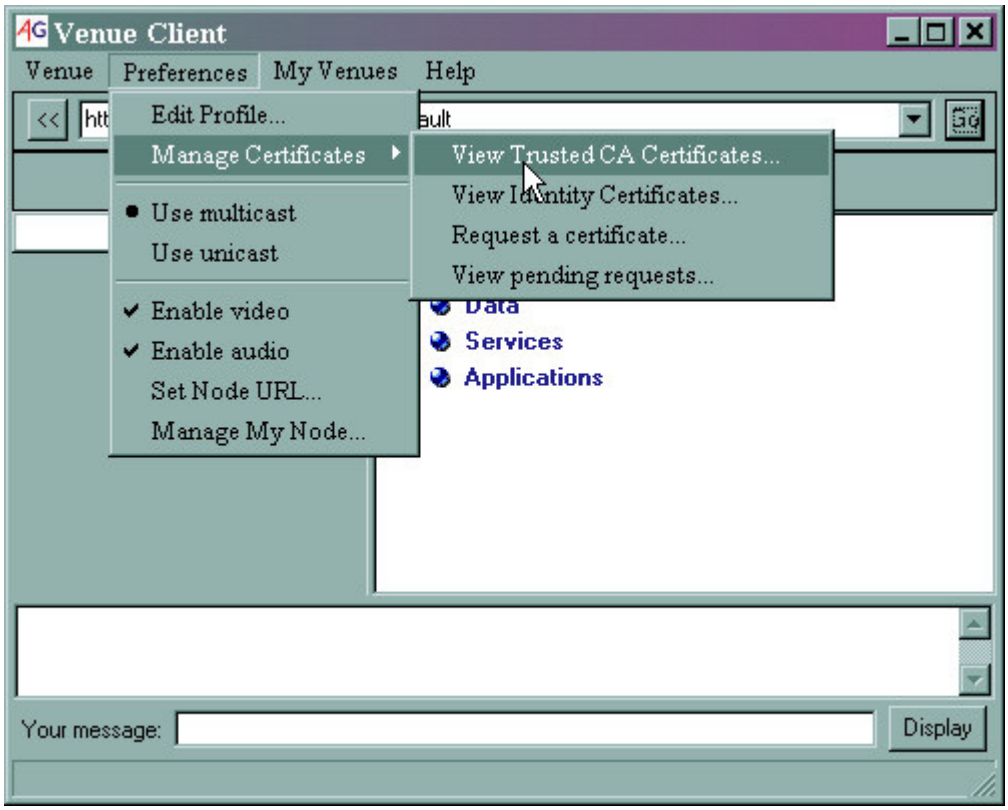

You can click on a name to see details about that identity:



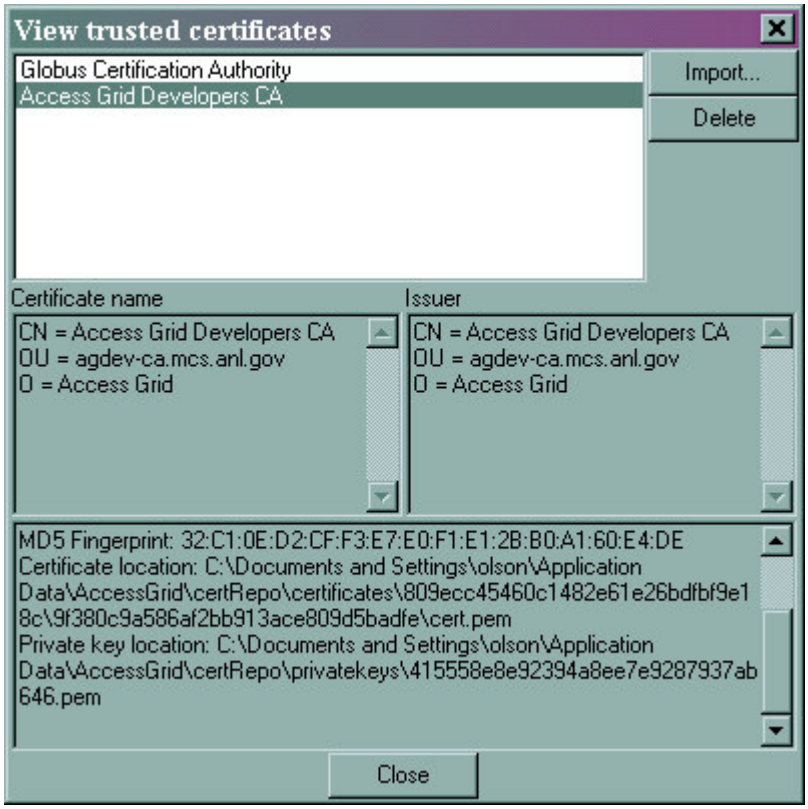

One identity is marked *(DEFAULT)*. This is the identity from which a Globus proxy will be created. To change the default, select an identity and press *Set as default identity.*

## Importing CA Certificates

If you need to add to the set of trusted CA certificates, you may do so in a process very similar to that of importing identity certificates. Open the trusted CA certificate browser:




You will see this dialog:



To import a new certificate, press *Import* and browse to the PEM-formatted CA certificate. You will also have to supply a Globus signing policy file, normally named the same as the CA certificate but with a suffix of .signing_policy.