Obtaining UK e-Science Certificates
Version 0.3

M. H. Eres
Hakki.Eres@soton.ac.uk
Southampton Regional e-Science Centre
School of Engineering Sciences
University of Southampton
Highfield, Southampton SO17 1BJ
United Kingdom

You need to apply to the UK e-Science Certificate Authority to obtain digital certificates in order to access CEDCs new Geodise toolkits and Globus servers. Everything is done by using a browser like Firefox or Internet Explorer (This document assumes Internet Explorer 6 is used).

Please use a browser running on your personal computer, not on a public workstation. After you finish your application, you need to use the same computer and the same browser to retrieve your certificate bundle.

Here are step-by-step instructions for obtaining personal Grid certificates from the UK e-Science Certificate Authority (CA).

1. Please read the documentation if you need to know further details.
   `http://www.grid-support.ac.uk/ca/documentation.htm`
2. Load the CA's root certificate to your browser:
   (a) Connect to `https://ca.grid-support.ac.uk/`
   (b) Click "View Certificate" on the "Security Alert" window.
   (c) Click "Install Certificate" on the "Certificate" window.
   (d) Click "Next" at the "Certificate Import Wizard" window.
   (e) Make sure "Automatically select the certificate store . . . " is selected, then click "Next".
   (f) Click "Next" at the "Certificate Import Wizard" window.
   (g) Click "Finish" at the "Certificate Import Wizard" window.
   (h) Click "OK" at the "Certificate Import Wizard" window.
   (i) Click "OK" at the "Certificate" window.
   (j) Click "Yes" at the "Security Alert" window.
3. After you have installed the CA's root certificate, click "Request a Certificate" link at the top of the page.

4. The Web server recognizes the browser you are using. And, if you are using an incompatible browser it won't accept your request.
5. If the server accepts your browser, click "User Certificate".
6. Fill in the form correctly. Choose "Southampton SeSC" as your registration authority (RA), not "Southampton NOC".
7. Enter your PIN and record it somewhere. This is not your Grid passphrase, it is merely used for the RA to identify you later.
8. When you are done, click "Continue".
9. Double-check your certificate request and if everything is fine click "Continue".
10. Click "Yes" at the "Potential Scripting Violation" window. (Depends on your browsers security settings).
11. Click "OK" at the "Creating a new RSA exchange key" window. (Depends on your browsers security settings).
12. Click "OK" at the "VBScript" window. (Depends on your browsers security settings).
13. Please read the certificate request confirmation page carefully.
14. If you would like to check the status of your certificate request, click on the "Requests Lists" tab, and then "Certificate Requests" link.
15. In couple of days you will receive an e-mail from the Southampton RA, and they will ask you to come over to ISS, fill out a form, show your ID, so that they can confirm your identity and forward your request back to the UK e-Science CA.
16. In a day or so, you will receive an e-mail with your certificates serial number from the CA. Now you can download your certificate to your browser. Please follow the following steps:
    (a) Connect to `https://ca.grid-support.ac.uk/`
    (b) Click "Import Certificate into Browser",
    (c) Enter your certificates serial number, and click "OK".
    (d) Click "OK" at the message window,
    (e) Click "Open" at the "File Download" window.
    (f) Click "Install Certificate" at the "Certificate" window.
    (g) Click "Next" at the "Certificate Import Wizard" window.
    (h) Make sure "Automatically select the certificate store . . . " is selected, then click "Next".
    (i) Click "Finish" at the "Certificate Import Wizard" window.
    (j) Click "OK" at the "Certificate Import Wizard" window.
    (k) Click "OK" at the "Certificate" window.

17. At this point, your personal certificate is loaded to your browser. Please follow the following steps to export it to a certificate bundle file:

    (a) Do "Tools"-"Internet Options"-"Content"-"Certificates" in Internet Explorer, and select your personal certificate.

    (b) Click "Export" at the "Certificates" window.

    (c) Click "Next" at the "Certificate Export Wizard" window.

    (d) Select "Yes, export private key" and click "Next".

    (e) Make sure "Personal Information Exchange ..." and only "Enable strong protection ..." is selected and click "Next".

    (f) Enter your export password twice, and click "Next".

    (g) Click "Browse", locate the directory of the certificate bundle file, enter a filename (e.g. `mybundle`) for the certificate bundle, and click "Save".

    (h) Click "Next".

    (i) Click "Finish".

    (j) Click "OK" at the message window.

    (k) Click "Close" at the certificate window.

    (l) Click "OK" at the "Internet Options" window.

18. Your UK eScience certificate bundle, which you have exported from Internet Explorer to be converted to PEM format. You need to copy it to `utp-10` (or any other Linux system with openssl installed) and follow the instructions below (from CA's help files):

    (a) If you want to use your certificate with Globus, you will have to convert the exported certificate to a different format. This section assumes you are using UNIX and have OpenSSL, and that the openssl command is in your path. We also assume you have stored your certificate with its private key in the file "mybundle.pfx". You will have to type your passphrase (the one that protects your private key) while running these commands.

    (b) For your personal certificate type

    ```
    openssl pkcs12 -in mybundle.pfx -clcerts -nokeys -out usercert.pem
    ```

    and supply your export password.

    (c) For your personal key type

    ```
    openssl pkcs12 -in mybundle.pfx -nocerts -out userkey.pem
    ```

    and supply your export password.

    (d) If you converted a personal certificate, openssl will ask you to type a (possibly different) passphrase - since your private key is exported now, you will have to provide a passphrase here to protect it. You must type it twice to ensure that you have not made a mistake.

(e) You now have your certificate in the file "usercert.pem" and your private key in "userkey.pem", for a user certificate. If you want to use the user certificate files with Globus, put them in your `~/.globus` directory, and do the following:

```
cd ~/.globus
chmod 400 userkey.pem
chmod 444 usercert.pem
```