Requesting a certificate using the eCMT application

Introduction

eCMT is the ePharmacy Certificate Management Tool. An electronic certificate is installed on each pharmacy system that sends messages to the ePharmacy message store. The certificate is required to ensure security across the ePharmacy infrastructure. It does two jobs: it ensures that messages are encrypted and secure as they are transmitted electronically, and it ensures that only authorised systems can send messages. Certificates are currently installed on your system – they were installed by your PMR supplier when they first set you up for eMAS.

To ensure continued security, the certificates periodically require renewal. To make this a simple process, your PMR supplier has installed the eCMT on your system. Please remember that your PMR suppliers only have responsibility for installing the tool. Any support on the tool can be provided via the PSD helpdesk on 0131 275 6600.

The certificate renewal process requires you to know your EPOC number and a PIN which will be sent to you in a letter similar to your bank PIN letters. The PSD helpdesk can provide you with your EPOC number if you don't already know it. When you receive your PIN letter, you will have two weeks to request and download the certificate. If this is not done in time, there is a risk that your current certificate will expire and you will be unable to send electronic messages to the ePharmacy message store.

After receiving your letter, follow the instructions below to request and install your certificate. The certificate request should be made by a person who is logged in with Administrator Privileges on the local machine.

Starting the eCMT application

On the Windows 'Start' menu select

All Programs -> ePharmacy Certificate Manager -> ePharmacy Certificate Manager

The following splash screen will appear, and the eCMT updater will attempt to contact the eCMT Web Service.

NB – the version number may be different.

If, for any reason, the eCMT Updater cannot contact the eCMT Web Service, an error message will be displayed. Otherwise, the eCMT Updater will begin checking for any available updates for the Application itself, or any new or revoked Certificates

Update Status – Checking for updates

At launch, the application will contact the Certificate Management Web Service to check if there are any available updates regarding the application itself or ePharmacy related Certificates.

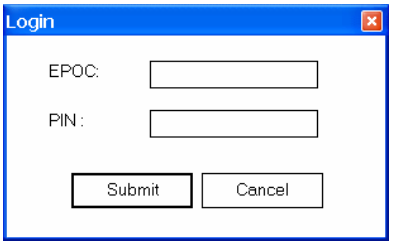
Should any updates be available, information detailing the type of update and the available user options regarding the update will be displayed.

The Welcome screen

Once the eCMT application has started, the following Windows dialog box is displayed.

Logging In

Click on the **Logon** button on the Welcome Screen.
The following windows Dialog is displayed.



Type your EPOC number and the associated PIN into the appropriate boxes.

Click on the '**Submit**' button.

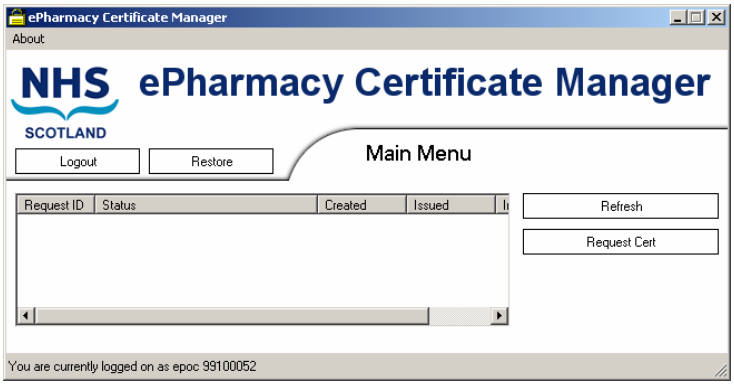
If the EPOC and PIN are valid, the Logon successful dialog box will be displayed.

Click **OK**.

The main eCMT application screen is displayed.

ePharmacy Certificate Manager Main Menu screen

The Main Menu screen allows users to manage and review Certificate Requests.

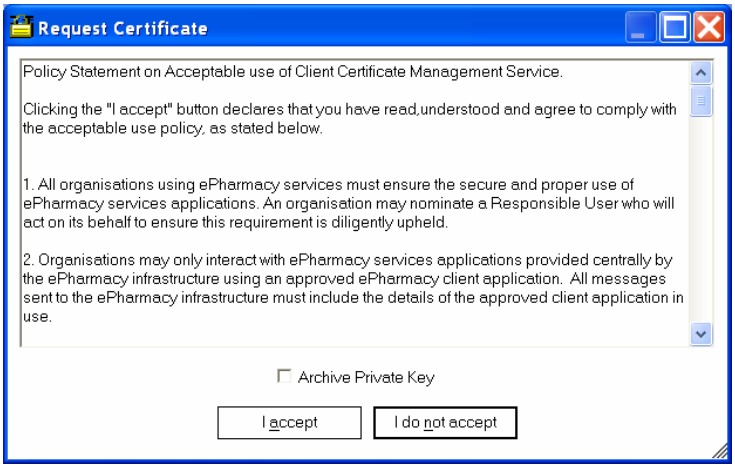


The status pane of provides details of each request that has been submitted.

Creating a Certificate Request

Requesting a Certificate

Click on the '**Request Cert**' button. The following Dialog Box will appear.



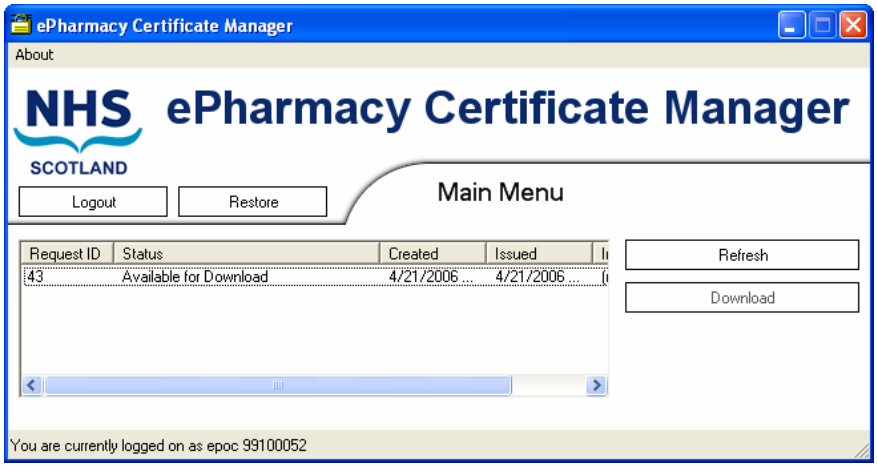
Do not check the 'Archive Private Key' checkbox. This functionality is now redundant and the checkbox will be removed in the next version of the eCMT.

Click on the '**I accept**' button.

CA Response to a Certificate Request

Certificate Request Authorised

Once a Certificate Request has been authorised by the CA, it will be shown in the status pane of the Main Menu window as 'Available for Download', as shown below.



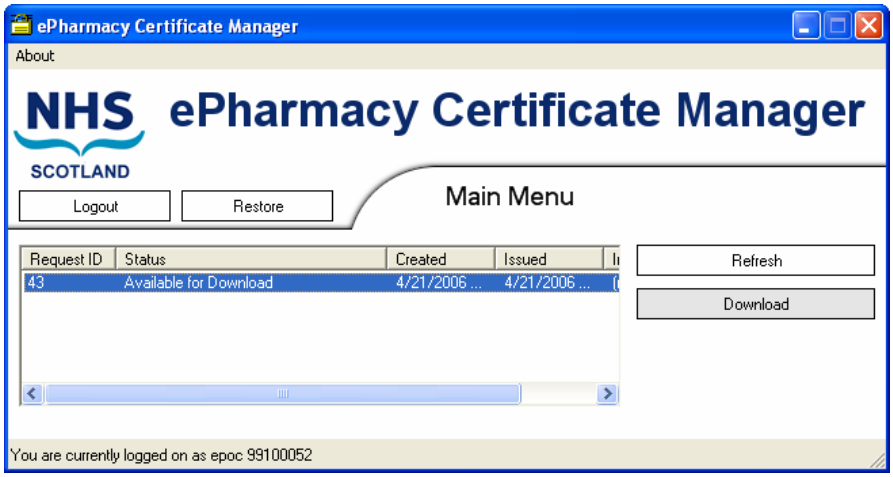
Certificate Request denied

In certain circumstances, a Certificate Request may not be authorised by the CA. If this is the case, it will appear in the Status pane of the Main Menu window with a status of ‘Denied’,.

Should a request be denied, users should contact the PSD helpdesk to resolve the situation.

Downloading a Certificate

A certificate request with a status of ‘Available for Download’ can be downloaded.
Click on the relevant entry in the Request Status table to highlight the entry for the Certificate to be downloaded, as follows.



Be sure to click on the correct request line in the status pane - there may be more than one entry in the request list.

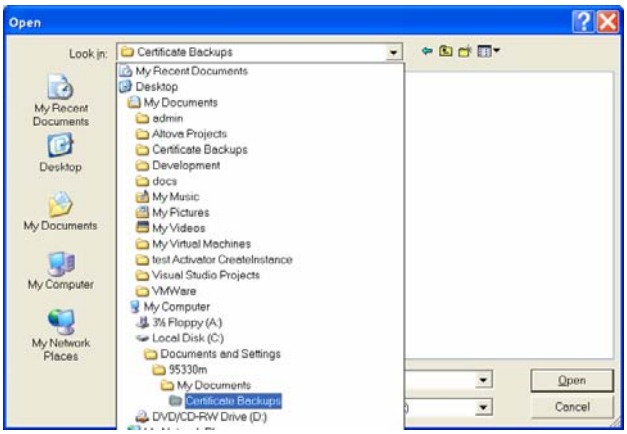
Click on the ‘**Download**’ button.

Installing a Certificate

When the ‘**Download**’ button has been clicked for an ‘Available for Download’ certificate request, the ‘Backup Certificate’ dialog box will be displayed, as follows.

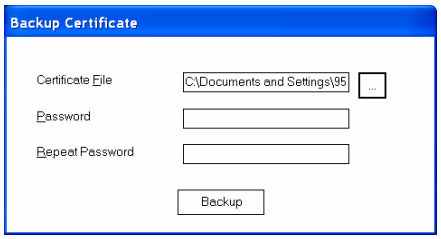
Select the Certificate File location

Click on the ellipsis ('…') button. A windows 'Open' dialog box will appear. Use the 'Look in' drop down control to browse to an appropriate location to save the backup file to, as shown in the following diagram.



Enter an appropriate name for the file in the 'File name' box. The application will automatically add the '.pfx' file extension- See below.

Click on the 'Open' button to set the path and filename for the certificate backup File. The 'Backup Certificate' dialog box will reappear, with confirmation of the path and filename in the 'Certificate File' text box.



Enter a suitable password in the 'Password' text box.
The password must:

- Be more than six characters long.
- Contain
  at least one upper case character (A, B, C …X, Y, Z),
  at least one lower case character (a, b, c … x, y, z), and
  at least one numeric character (0, 1, 2, … 7, 8, 9).

As confirmation, type exactly the same password in the 'Repeat Password' textbox. Safe and secure storage of the password is entirely the responsibility of the User. The password is not stored elsewhere in the application and so cannot be recovered. The certificate cannot be restored from this backup file without the password.

Click on the 'Backup' button to backup the certificate. Remember to copy the backup file to a

secure backed up area on the server so that a copy will still be available in the event of a server failure. Your PMR system supplier will be able to confirm which areas are backed up.