NHSScotland ePharmacy Delivery

ePharmacy Certificate Manager Installation / User Guide

EPD-US/UG/UG003

Version: 1 Final

15/9/2006

Contents

1. Introduction

1.1 Document Purpose

This document describes how to install and use the ePharmacy Certificate Manager application. It also acts as a “How to guide” to help you when you have a problem regarding certificates used for ePharmacy.

1.2 Overview of Certificates within the ePharmacy system

1.2.1 What are Certificates and why are they needed?

In everyday life, we are used to the idea of using a passport as a means of identification. We also have credit cards that have spending limits, and driving licences that specify the type of vehicle we are authorised to drive.

In the world of ePharmacy, the task of establishing identity and authorisation is achieved using digital certificates. These Certificates are installed onto individual computers and then used to identify them on the network. Based on the ‘identity’ of a given Certificate, specific levels of access and authorisation are given to the computer when communicating with the ePharmacy system.

Note - without a valid Certificate, it is not possible to access the ePharmacy system.

1.2.2 Who needs a Certificate?

Whereas passports and driving licences are issued to individuals, digital certificates are issued to ‘Message End Points’ – usually a physical location such as an individual Practice or Pharmacy. In some cases, a Message End Point may correspond to an individual user with a single computer, but in others several computers may form a single Message End Point. Whether consisting of one or more computers, each Message End Point accesses the ePharmacy system using the ‘identity’ of a single Certificate. This identity is associated with a unique number (an ‘EPOC Number’) that is contained as part of the certificate.

1.2.3 Who is Responsible for a Certificate?

A parent can have their own passport, but in the eyes of the law is also responsible for passports issued to their children. Similarly, each Message End Point has a designated Responsible Person who is in charge of managing the Certificate not only for their computer, but also for Certificates on any other computers within their group.

The Responsible Person is also the point of contact for any correspondence

associated with ePharmacy system access and use.

1.2.4 Who issues a Certificate?

A digital Certificate is issued by a Certification Authority (CA). The ePharmacy delivery team maintain a dedicated CA, purely for use by the ePharmacy system.

In addition to the unique Certificate issued to the Responsible Person at each Message End Point, the CA also issues a special, shared, 'Root' Certificate which is used to identify the ePharmacy CA as the issuer of the unique Certificates.

1.2.5 How do I contact the Certification Authority?

The Responsible Person for each Message End Point will be sent the necessary information and instructions, including a unique identification number for that Message End Point. In addition, a 'secret' PIN Number that is known only to the system and the recipient will be sent – similar to the PIN number that is sent when a new credit card or bankcard is issued.

Note: As with other systems that use PIN Numbers, entering the PIN incorrectly three consecutive times will result in the account being 'locked out'. This will consequently require contact with the PSD helpdesk (see section 5.1.1.1 for contact details) to reopen the account.

1.2.6 How long does a Certificate last?

A Certificate has an expiry date, after which it must be renewed. As with a credit or bankcard, the term 'renewed' actually means a new item is created and issued to the user as a replacement for the original one. The ePharmacy system still maintains information that the old Certificate existed, and about how and when it was used, but the original is now invalid.

1.2.7 What is involved in 'managing' a Certificate?

Over the life of a Certificate, a number of events need to be managed. As with passports and credit cards, it is necessary to make a request before being issued with a Certificate. Although it is a 'digital' Certificate, it does physically exist. Accordingly, it can be lost or damaged, or even 'stolen' or compromised in some way.

As its name implies, the purpose of the ePharmacy Certificate Manager application is to assist a designated Responsible Person with all aspects of managing certificates. This includes initially requesting a certificate, installing it onto the computer(s) at a Message End Point, keeping the Certificate secure, and making any scheduled and unscheduled updates that are required.

1.2.8 Who manages the Certificate ?

The Responsible Person may choose to delegate the actual Certificate management tasks to someone else, but cannot transfer the obligations and responsibilities associated with the role.

Whoever actually performs the tasks must have specific rights and privileges on the necessary computer(s), as detailed in Section 5.2.

1.3 ePharmacy Certificate Manager Overview

1.3.1 Installing the ePharmacy Certificate Manager application

1.3.1.1 Initial installation of the application

Before it can be used to manage Certificates, the Client Certificate Manager application must itself be installed on at least one computer at each location. This is typically the computer that has ePharmacy adapter software installed.

See section 2.1.2.1 for details of installing the application from the Internet, or section 2.1.2.2 has details of installing the application from CD.

1.3.1.2 Updates to the application

Each time the application is started, it checks for updates available from a dedicated ePharmacy web service. This includes checks for a new version of the application itself, and for new or revoked Certificates. See section 4 for details of this automatic update process.

1.3.2 Using the ePharmacy Certificate Manager application

The application can be used to assist in the following activities during the ‘lifetime’ of a certificate.

1.3.2.1 Requesting a certificate

Before accessing the ePharmacy system, the Responsible Person for each Message End Point must initially request a certificate from the ePharmacy Certification Authority (CA). Section 3.2 has details of how to Request a Certificate

1.3.2.2 Checking the Status of a Certificate Request

Once a Certificate has been requested using the application, the application will monitor the status of the Certificate throughout its lifetime, showing whether the Certificate is pending, approved, installed, or requires replacement.

Section 5.3 has a full list of all possible status messages.

Once logged in to the application, the main Menu window shows the status of all Certificate Requests – see section 3.1.3.1.

1.3.2.3 Requesting that the CA makes a Certificate backup

When a certificate is available for download, users can request that the ePharmacy CA make a backup of their certificate. This will allow a request for a replacement Certificate to be made should this become necessary for whatever reason, e.g. replacement of PC, disc crash, etc.

1.3.2.4 Installing a Certificate

Once the Request has been received and subsequently authorised, the Certificate may be downloaded from the CA. The Certificate can then be installed onto each computer that will access the ePharmacy system.

Section 3.4 gives details of the installation procedure.

1.3.2.5 Copying a Certificate

All computers within a Message End Point share the same identity when accessing the ePharmacy system. Accordingly, the appropriate Certificate must be copied on to any other computers that require it.

In addition, the Responsible Person may wish to have a local copy of a Certificate as part of their local computer maintenance policy.

Section 3.4 covers copying a Certificate within the local computer environment.

1.3.2.6 Restoring a Certificate

If the eCM application has been used to make a local copy of a Certificate, the application can be subsequently used to restore the Certificate from the local copy.

Section 3.7 covers this restoring a Certificate from a local copy.

1.3.2.7 Reinstalling a Certificate

If, at the time of downloading a Certificate, the Responsible Person requested that the CA stored a copy the Certificate, the application can be used to reinstall a Certificate from this CA copy.

Section 3.8 covers reinstalling a Certificate from a CA backup copy.

1.3.2.8 Renewing a certificate

Prior to a Certificate reaching its expiry date, the Responsible Person will be sent a new PIN number. Using this new PIN number, the eCM application can be used to request a replacement certificate. This renewal will occur before the existing Certificate expires. Section 3.5 covers requesting that a Certificate may be

renewed.

2. Installing the eCM application

2.1 Installation

This section covers initial installation of the eCM application.

The installation programme uses a 'wizard' (i.e. a sequence of Windows dialog boxes) to collect the information it needs and at the same time guide you through the installation.

Note - A user must have the necessary access permissions to install the application – see section 5.2.2.1. for details of the required permissions.

2.1.1 Accessing the setup wizard

The eCM Installer is available either

- from the web. See section 5.1.2 for details on how to obtain access.
- on CD. See section 2.1.2.2 for details on how to obtain access.

2.1.2 Launching the setup wizard

2.1.2.1 Launching from the web

www.eps.nds.scot.nhs.uk/eCM/CertificateManagement.Setup.msi

See 2.1.3 to continue.

2.1.2.2 Launching from CD

Refer to your GP or Pharmacy System Software Supplier's documentation (as appropriate) to locate the eCM application installation program.

Double click on the 'CertificateManagement.Setup.msi' Icon.

2.1.3 Setup Wizard Welcome Screen

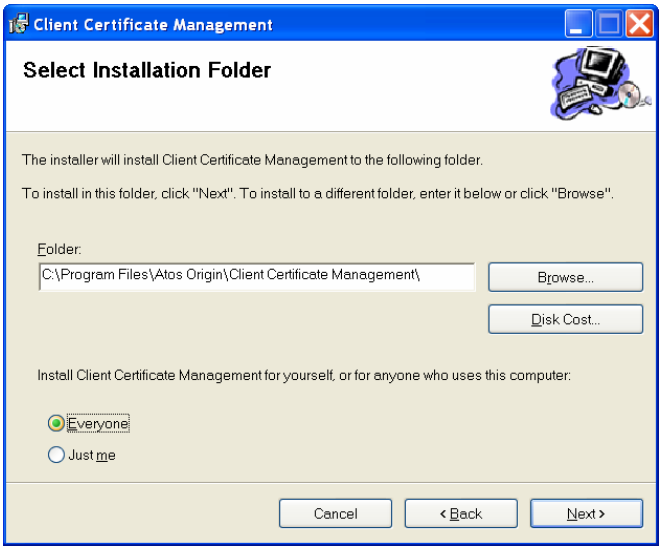
When the wizard starts, the following Windows dialog box will be displayed.

Click on the *'Next>'* button to proceed with the installation.

If for some reason you do not wish to continue with the installation, click the *'Cancel'* button to abandon installation.

2.1.4 Selecting the Installation Folder

The following Windows dialog box is displayed.

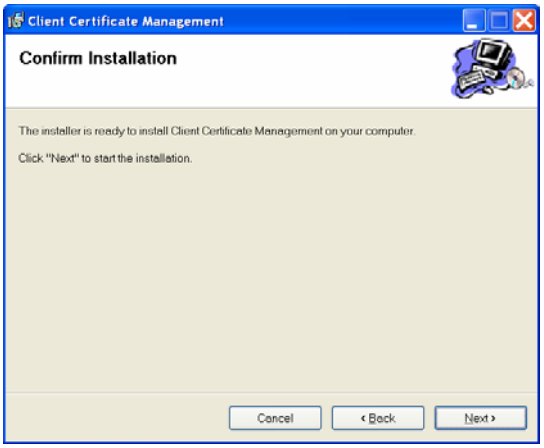


Click on the *'Next>'* button to accept the default installation directory (recommended), or follow the instructions on the dialog box to specify an alternative installation directory before clicking the 'Next>'button.

(Alternatively click on the *'<Back'* button to return to the previous screen, or click on the *'Cancel'* button to abandon installation.)

2.1.5 Confirming Installation

The following Windows dialog box is displayed.

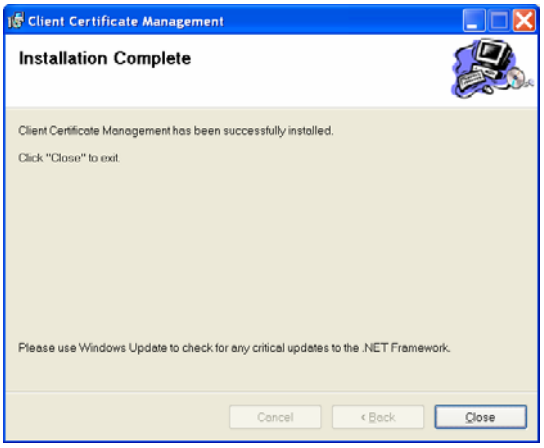


Click on the *'Next>'* button to continue the installation.

(Alternatively click on the *'<Back'* button to return to the previous screen, or click on the *'Cancel'* button to abandon installation.)

2.1.6 Completing Installation

On successful completion of the installation, the following Windows dialog box is displayed.



Click on the *'Close'* button to complete the installation and begin using the eCM Client Application.

3. Using the eCM application

3.1 Starting the eCM application

Once the application has been installed, on the Windows 'Start' menu select

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

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

Note – the version number may be different.

If, for any reason the eCM Updater cannot contact the eCM Web Service, an error message will be displayed – see 5.4.1 for more details. Otherwise, the eCM Updater will begin checking for any available updates for the Application itself, or any new or revoked Certificates

3.1.1 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. See section 4 for further details of the update process.

3.1.2 The Welcome screen

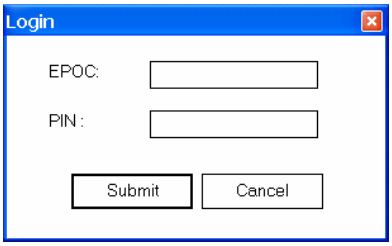
Once the eCM application has started, the following Windows dialog box is displayed.

Note, it is not necessary to log on to restore a previously saved Certificate using the eCM application - see section 3.7 for details of the restore operation.

3.1.3 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. The EPOC Number and PIN are included in the Supplied Documentation to ePharmacy users – see section 0

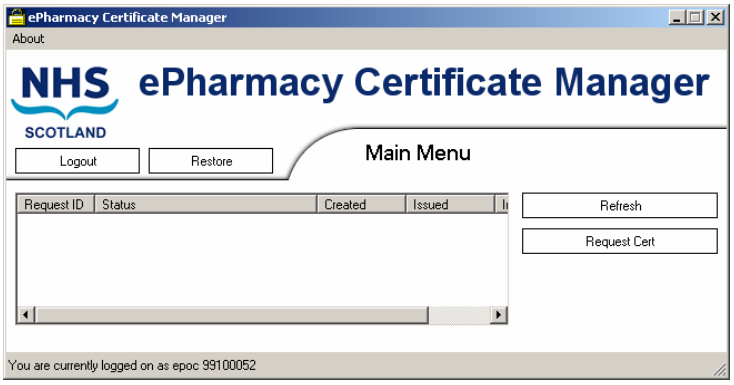
Click on the 'Submit' button to access the eCM Client Application for the given EPOC Number.

(Alternatively, click the 'Cancel' button to abandon logon and return to the Welcome Screen).

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

Click OK.

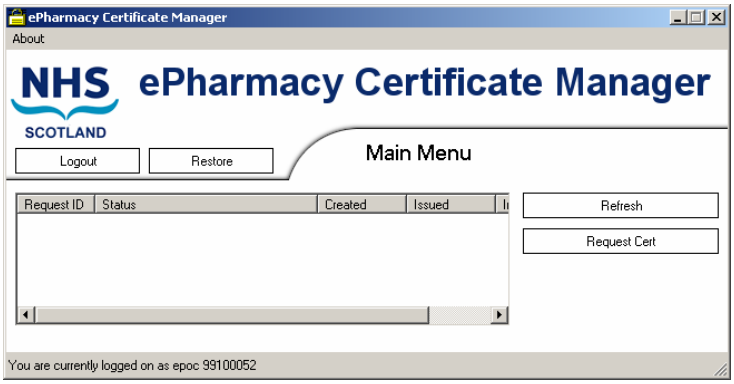
The main eCM application screen is displayed.



(If there is a problem with the entered EPOC or PIN, an error message will be displayed – see section 5.4.2 for details of possible errors and their resolution.)

3.1.3.1 ePharmacy Certificate Manager Main Menu screen

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

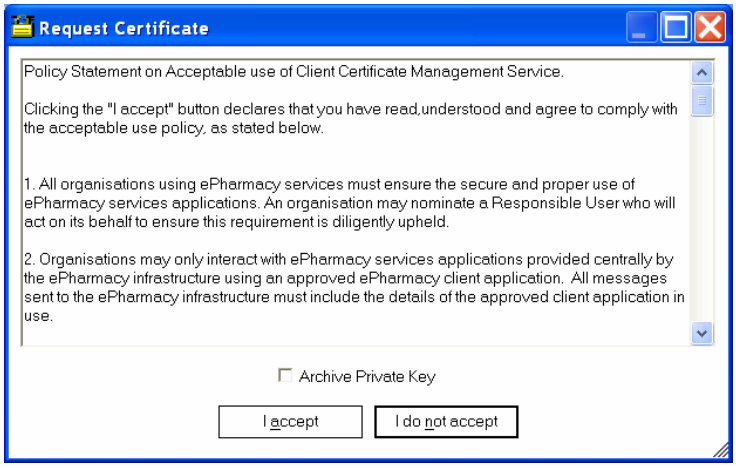


The status pane of provides details of each request that has been submitted. See section 5.3 for a list of possible status indicators, together with an expanded explanation of each indicator.

3.2 Creating a Certificate Request

3.2.1 Requesting a Certificate

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



If the requested certificate is to have the private key archived, then ensure the 'Archive Private Key' box is checked.

By checking the 'Archive Private Key', the eCM user is requesting that the ePharmacy CA makes a copy of the Certificate and stores this copy on the CA computer on behalf of the user. This would allow the user to request retrieval of this copy at some time in the future, should the original Certificate be lost (as opposed to requesting a new, replacement Certificate). The 'CA archived' copy cannot be used to replace a Certificate that has expired or otherwise become invalid.

Click on the *'I accept'* button. Section 5.2 has details of obligations accepted by clicking on this button.

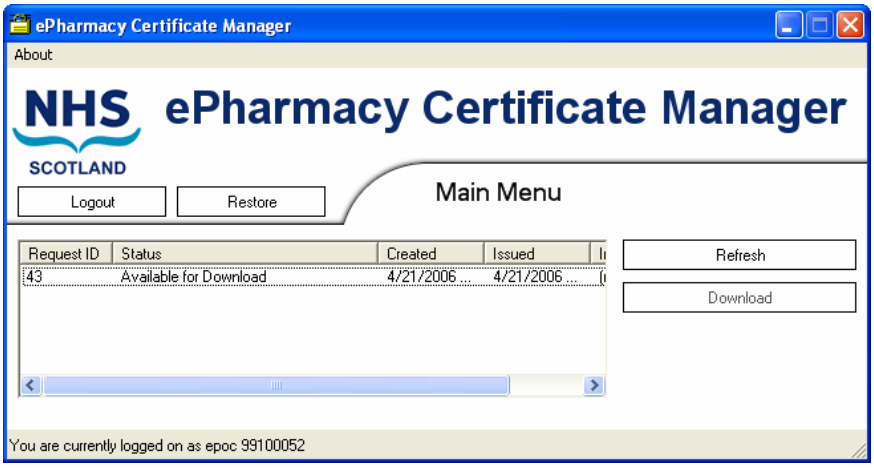
3.2.2 CA Response to a Certificate Request

3.2.2.1 Request Pending

A request that has been submitted, but not yet authorised by the CA, will be shown with a status of 'Under Submission' in the Main Menu window status pane.

3.2.2.2 Certificate Request Authorised

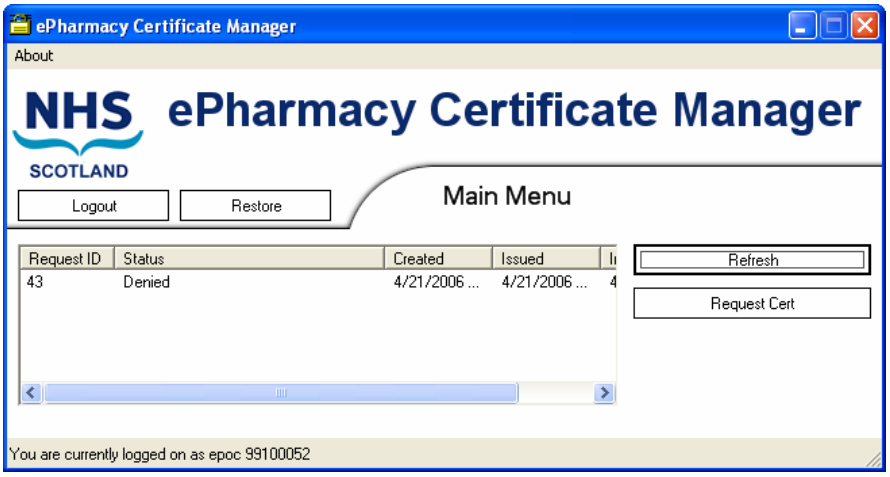
Once a Certificate Request has been authorised by the CA, it will be shown in the status pane of the Main Menu window as 'Available for Download', as shown below.



A Certificate request with a status of 'Available for Download may be downloaded using the steps detailed in section 3.3.

3.2.2.3 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', as shown below.



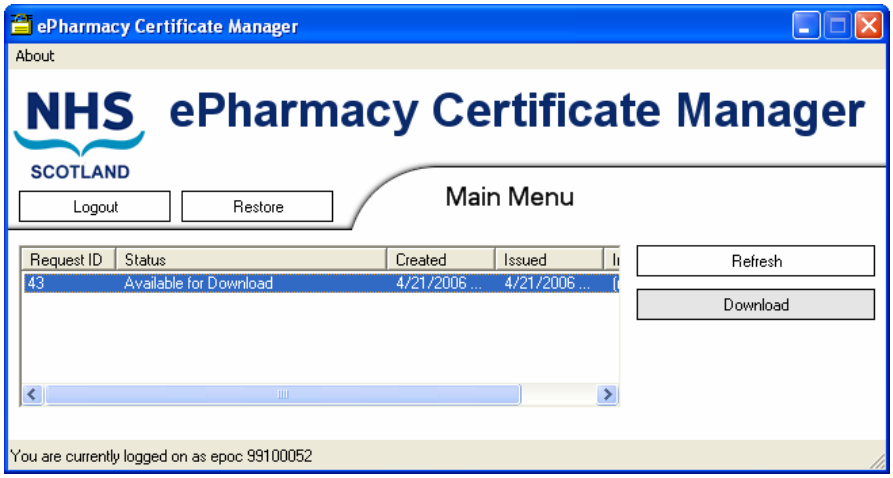
Should a request be denied, users should contact the PSD helpdesk to resolve the situation – see section 5.1.1.1.

3.3 Downloading a Certificate

Note – The person who downloads the Certificate should be the same person who requested the Certificate, and should be logged onto the local system using the same Windows Account (i.e. Windows Username) that was being used when the Certificate request was made. This person should have Administrator Privileges on the local machine.

If a certificate request has a status of 'Available for Download', it 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.

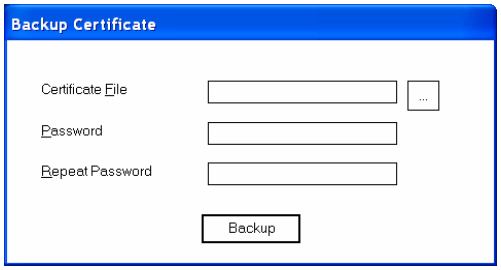


Be sure to click on the correct request line in the status pane - there may be more than one entry in the request list.

Click on the *'Download'* button.

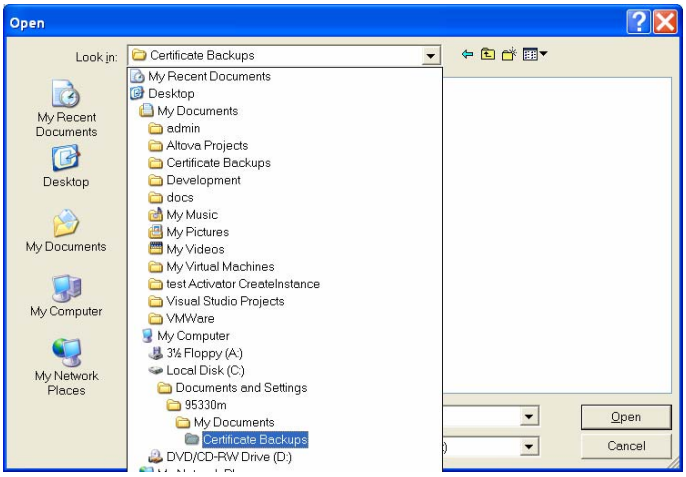
3.4 Installing a Certificate

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

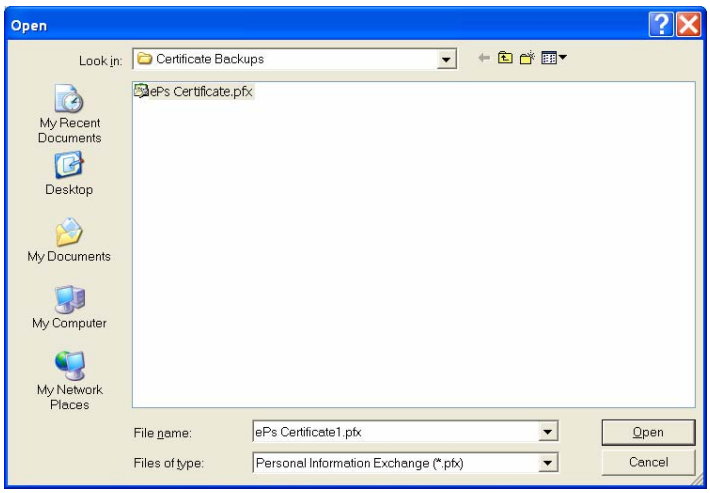


3.4.1 Select the Certificate File location

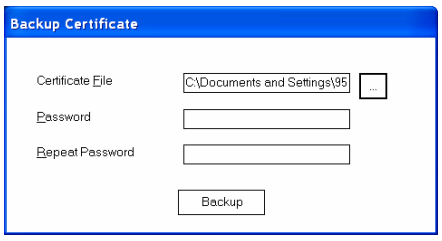
Click on the ellipsis ('…') button. A windows 'Open' dialog box will appear. Use the 'Look in' drop down control to browse to an appropriate location to save the backup file to, as shown in the following diagram.



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.

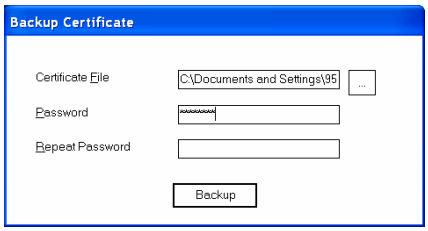


Enter a suitable password in the *'Password'* text box.

Note – The password must

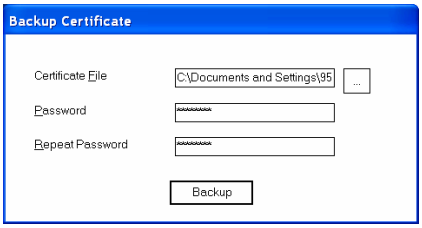
- Be more than six characters long.

- 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).



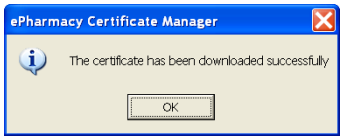
As confirmation, type exactly the same password in the *'Repeat Password'* textbox.

Note: 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.

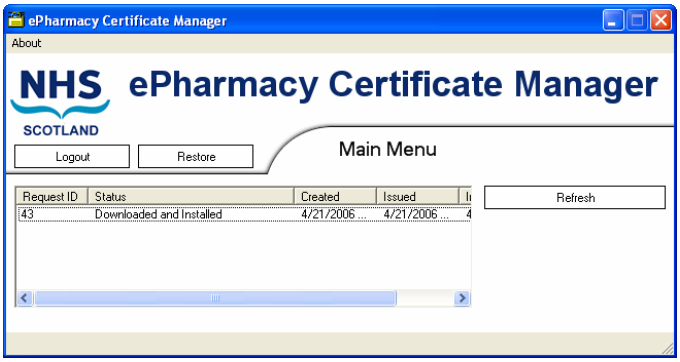


Click on the 'Backup' button to backup the certificate.

If successful, the following dialog box will appear.



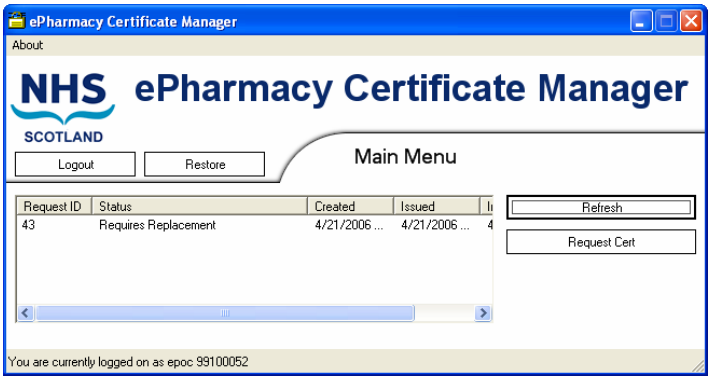
Click on the *'OK'* button to continue. The Main Menu window will appear, this time showing the status of the certificate as 'Downloaded and Installed'.



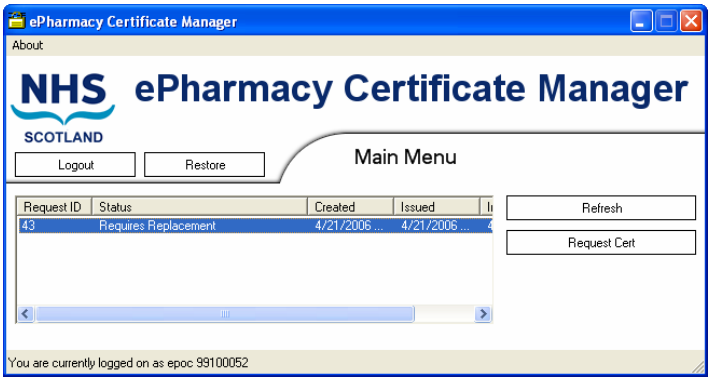
3.5 Renewing a Certificate

All EPOC Certificate requests made through the eCM Client application have their status shown in the Main Menu window of the eCM Client Application. When an EPOC Certificate is about to expire its status will be shown as 'Requires Replacement'.

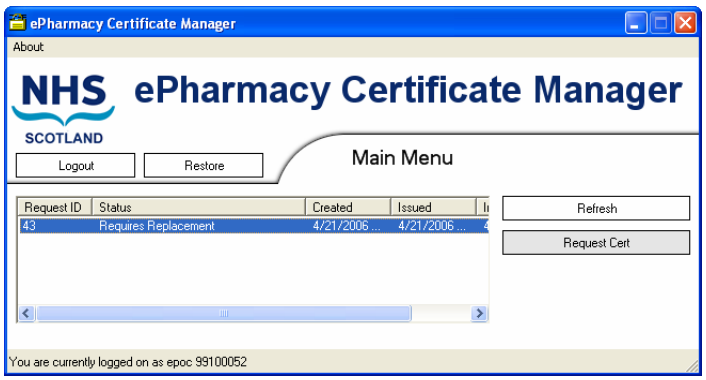
At this time a letter will be sent to the Responsible Person advising that the Certificate is due for replacement, and which will include a new PIN Number.



Click on the appropriate Request entry in the Main Menu list to highlight that request and enable the *'Request Cert'* button.

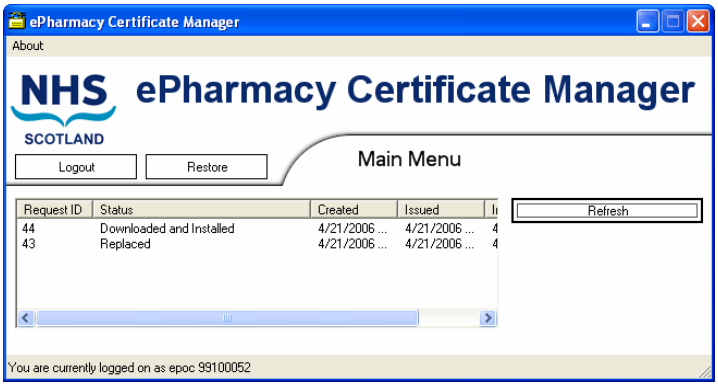


Click on the *'Request Cert'* button.



See section 3.4 for details of downloading and installing the new Certificate.

The status of the Request will change to ‘Replaced’.



Note. The original EPOC certificate is not removed from the Client machine.

3.6 Removing a Revoked Certificate

Revoked Certificates are detected by the eCM Client Application Updater, which runs automatically when the eCM Client Application is launched. See Section 4

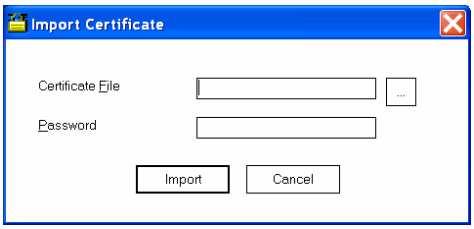
3.7 Restoring a Certificate from local backup copy

Note – it is NOT necessary to log on to the eCM Client Application in order to restore a Certificate from local backup copy.

3.7.1 Restoring a previously backed up certificate

Click on the ‘Restore’ button on the Welcome or Main Menu Window.

The following Windows Dialog is displayed.



This screen is used to restore a certificate from a file that was previously backed up using the eCM Client application – see section 3.4.

Note – The User must know the name and location of the backed up file, and the back up Certificate password in order to use this functionality.

3.8 Reinstalling a Certificate from a CA Archive copy

The following procedure details the steps necessary to recover an ePharmacy account where the Certificate has been lost, but has previously been archived with the ePharmacy CA.

1. The Responsible Person phones the PSD Helpdesk, advising that the ePharmacy system can no longer be accessed – see section 5.1.1.1.

2. A new Certificate will be sent to the Responsible Person on a CD. NOTE: Delivery of a new Certificate will take a minimum of 3 working days.

3. The Responsible Person installs/restores the CD file of the Certificate using the eCM application restore function (section 3.7).

4. At this time, the Responsible Person phones the PSD helpdesk to request the Certificate password.

5. The Certificate is installed, and the ePharmacy system can again be accessed.

3.9 Certifcate Lost and not Archived with ePharmacy CA

The following procedure details the steps necessary to recover an ePharmacy account where the Certificate has been lost, but HAS NOT previously been archived with the ePharmacy CA.

1. The Responsible Person phones the PSD Helpdesk, advising that the ePharmacy system can no longer be accessed – see section 5.1.1.1.

2. The ePharmacy delivery team will re-enable the account and send out a new PIN .
   NOTE: Delivery of the new PIN will take a minimum of 3 working days.

3. Once the new PIN has been received, the Responsible Person logs into the eCM application.

4. The Responsible Person requests a new Certificate using the eCM application.

5. The Certificate request is authorised, the Certificate is installed, and the ePharmacy system can again be accessed.

4. eCM Updater

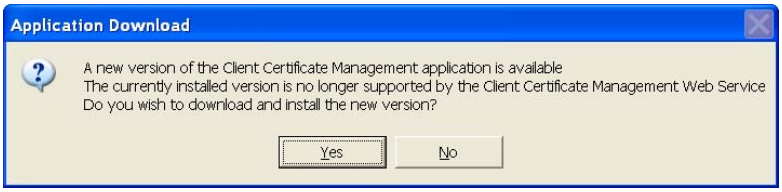
At launch, the eCM application checks the eCM Web Service for available updates. There are three possible types of update

- Updates to the eCM application itself (see section 4.1)
- New CA Root Certificates (see section 4.2)
- Revoked CA Root Certificates (see section 4.3)

Note – more than one update may be detected at the same time.

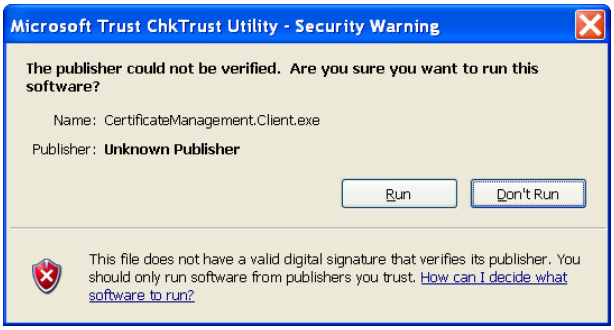
4.1 New Application version is available

This dialog is displayed when a new version of the eCM Client application is available for download from the eCM Web Server, and the currently installed version is no longer supported by the eCM Web Service.



4.1.1 Downloading and installing a new version of the eCM Client Application

Click the '*Yes'* button on the Application Download dialog.



Click the *'Run'* button to continue the download and installation (Alternatively, click on '*Don't Run'* to cancel the application download and proceed to step 4.1.2)

The current version is closed down, and the new version of the application is launched.

4.1.2 Skipping download and using existing application functionality

If the User clicked on the *'No'* button at step 4.1.1, the updater will proceed to check for Certificate updates being available from the eCM Web Service. Should one or more Certificate updates be available, the appropriate dialog will appear – see the subsequent sections of this chapter.

4.2 New Root Certificate(s) available for download and installation

The eCM Updater checks the web service for any newly available Root Certificate(s). If any are found, the following Windows Dialog is presented.

Note – The number of certificates found may vary.

Follow the instructions on the dialog to install the new version, or continue using the current version.

Note - this dialog will appear once for every new certificate

4.2.1 Installing a new certificate

Click the *'Yes'* button on the Certificate Download Windows dialog – section 4.2 above.

In the majority of cases the normal welcome screen is shown - see 3.1.2 for details of operation from that point.

However, if further certificate updates are also available, one of the dialogs shown in subsequent sections of this chapter will be shown.

4.2.2 Skipping new certificate installation

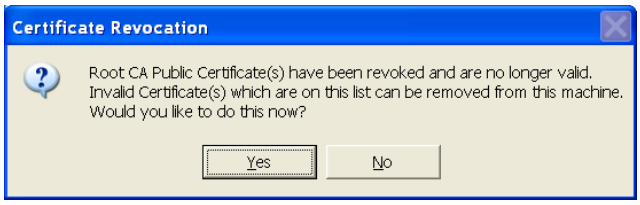
Click the No button on the Certificate Download Windows dialog – see section 4.2

Note – It is recommended that any newly available Certificates should be installed at the first opportunity.

4.3 Revoked Root Certificates

The eCM Updater checks the web service for updated information regarding revoked Root Certificates. If such information is presented by the Web Service,

the following Windows Dialog is presented.



Follow the instructions on the dialog to remove the old version, or continue using the current version.

Note - this dialog will appear once for every revoked certificate

4.3.1 Removing a revoked Certificate

Click on the '*Yes*' button on the Certificate Revocation windows dialog 4.3

4.3.2 Leaving a Revoked Certificate in place

Click on the '*No*' button on the Certificate Revocation windows dialog - see 4.3

Note – It is recommended that any newly revoked Certificates should be removed from the local machine at the first opportunity.

5. Reference

5.1 eCM Product Support

5.1.1 Contact Details

5.1.1.1 PSD Helpdesk

Telephone: 0131 275 6600

Email: psdhelp@psd.csa.scot.nhs.uk

5.1.2 eCM Application Download

www.eps.nds.scot.nhs.uk/eCM/CertificateManagement.Setup.msi

5.1.3 Supplied Documentation

An introductory letter, which will contain the PIN Number and be printed on secure paper, will be sent to the Responsible Person.

5.2 User Credentials and Authorisations

5.2.1 ePharmacy Permissions

The Responsible Person must have physical access to EPOC Number and associated PIN Number – see section 0.

5.2.2 Local Computer Permissions

5.2.2.1 Permissions required to install the eCM Application

The User must have the following local Windows permissions on the computer that the eCM Application is to be installed onto.

- Windows Administrator rights.

5.2.2.2 Permissions required to run the eCM Application

The User must have the following local Windows permissions on the client system to install the eCM Application.

- Read permission

- Write permission
- Delete permission

On the following Certificate Stores on the computer in question

- Trusted Root Certificate Authorities,
- Personal store
- Request store

5.3 Certificate Request Status Indicators

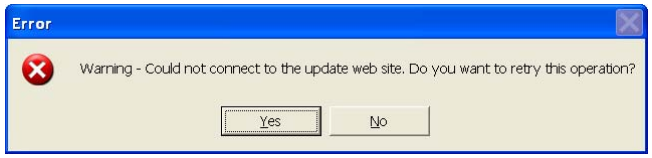
Status	Meaning
Incomplete	Request did not complete for some reason on the CA Server. Contact the PSD Help desk – see 5.1.1.1 for contact details.
Error	Error Occurred Creating request. Contact the PSD Help desk – see 5.1.1.1 for contact details.
Denied	The administrator of the CA denied the request - a User may submit another request.
Issued And Available For Install	Request has been accepted but has not yet been installed by the client.
Issued And Downloaded	Request has been accepted, downloaded but the install failed or a failure occurred in the transmission of the ePharmacy system message. Contact the PSD Help desk – see 5.1.1.1 for contact details.
Issued And Installed	Request has been accepted and installed by the client.
Issued Out Of Band	Contact the PSD Help desk – see 5.1.1.1 for contact details.
Under Submission	The request has been submitted by the Client and is on the CA awaiting approval by administrator.
Revoked	The request has been accepted and then revoked by the Certificate Authority.
Requires Replacement	The certificate is reaching its expiry date and should be replaced.
Replaced	The certificate has been replaced by another certificate.

5.4 Error Messages

5.4.1 eCM Web Service unavailable

5.4.1.1 Context:

If, when the eCM client Application is launched, the eCM Updater cannot contact the eCM Web Server, the following Windows dialog will be displayed.



5.4.1.2 Possible causes

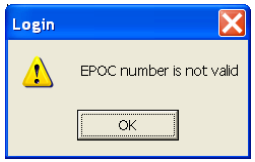
Error	***Cause***	***Resolution***
Network connection problem	Network problem or slow network connection temporarily restricting access to the eCM Web Service.	Click on the Yes button to attempt to re-connect to the eCM Web Service. If the error re-occurs, contact your system administrator/ISP.
Web Service is not available	Network connection and/or eCM Web Service unavailable to eCM Client Application.	Click on the No button to skip checking for updates from the eCM Web Service and continue using the currently installed version of the eCM Client Application and Certificates. The application will proceed to the Welcome Screen – see section 3.1.2.
Web Service offline.	eCM Web Service is offline or otherwise unavailable.	Contact PSD helpdesk for eCM Web Service status information – see section 5.1.1.1 for contact information.

5.4.2 Log On Failure

5.4.2.1 Invalid EPOC

5.4.2.1.1 Context

The EPOC number entered into the login screen (section 3.1.3) has not been accepted, resulting in the following Windows dialog being displayed.



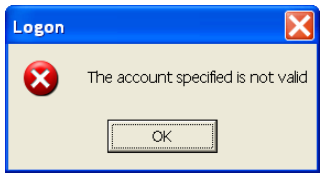
5.4.2.1.2 Possible causes

Error	***Cause***	***Resolution***
Data entry error	The EPOC number was incorrectly entered into the Login dialog.	Click on the 'OK' button to return to the login screen and to re-enter the EPOC number.
Invalid EPOC error	The EPOC does not exist within the eCM system, or the EPOC has expired, or the EPOC has been locked.	Check that the EPOC number is correct as detailed in the supplied eCM documentation. If the EPOC number previously entered does not match the number on the documentation, click on the 'OK button to return to the Login screen and enter the correct EPOC number. If the EPOC entered does match the documentation, but is not accepted, contact the PSD Helpdesk to have the EPOC included/unlocked - see section 5.1.1.1 for contact details. Otherwise, contact the PSD Helpdesk for further assistance - see section 5.1.1.1 for contact details.

5.4.2.2 Account not valid

5.4.2.2.1 Context

The EPOC number entered into the login screen (3.1.3 has not been accepted, resulting in the following Windows dialog being displayed.



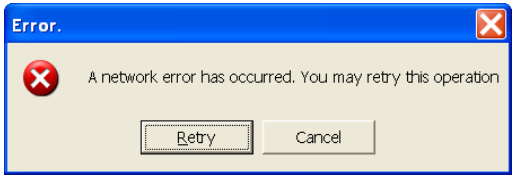
5.4.2.2.2 Possible causes

Error	***Cause***	***Resolution***
Data entry error	The PIN number was incorrectly entered into the Login dialog.	Click on the 'OK' button to return to the login screen and to re-enter the PIN number.
PIN does not match EPOC	PIN and EPOC are valid individually but are not together.	A PIN is only valid for a single EPOC. Contact the PSD Helpdesk for further assistance - see section 5.1.1.1 for contact details.
PIN is Invalid	The PIN does not exist within the eCM system, or the PIN has been locked.	Check that the PIN number is correct as detailed in the supplied eCM documentation. If the PIN number previously entered is not the PIN number on the documentation, click on the 'OK button to return to the Login screen and enter the correct PIN number. If the PIN entered does match the documentation, but is not accepted, contact the PSD Helpdesk to have the PIN included/unlocked - see section 5.1.1.1 for contact details. Otherwise, contact the PSD Helpdesk for further assistance - see section 5.1.1.1 for contact details.

5.4.2.3 Network error

5.4.2.3.1 Context

While a User is attempting to complete an action accessing the eCM Web Server, the following dialog box is displayed.



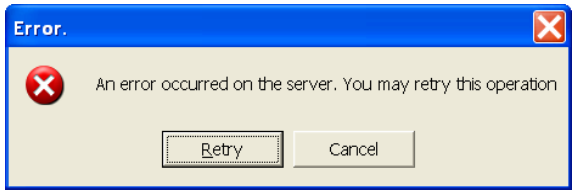
5.4.2.3.2 Possible causes

Error	***Cause***	***Resolution***
Network unavailable.	Momentary network failure/slow network connection.	Press Retry.
Network unavailable.	More permanent network failure.	Press Cancel. Contact the System Administrator/ISP who supports the Users system.

5.4.2.4 Server Error

5.4.2.4.1 Context

While a User is attempting to complete an action accessing the eCM Web Server, the following dialog box is displayed.



5.4.2.4.2 Possible causes

Error	***Cause***	***Resolution***
Process execution failure.	Failure within the eCM Web Service	Press Retry. If the error persists, contact the PSD help desk (see 5.1.1.1 for contact details) with details of the circumstances at the time the error occurred.