



Australian Government
Medicare Australia

*Installing a location certificate to enable access to HPOS
without prompting for a password at each log in*

User Guide for Windows XP
(Release date: June 2009)

eBusiness service centre: 1800 700 199
Email: onlineclaiming@medicareaustralia.gov.au

www.medicareaustralia.gov.au

Table of Contents

Introduction	2
Location Certificate install	2

Table of Figures

Figure 1: Index html page	3
Figure 2: Run	4
Figure 3: Run explorer	4
Figure 4: Windows explorer	5
Figure 5: Windows Explorer CD Drive	5
Figure 6: CD Content icon view	6
Figure 7: Changing to details view	6
Figure 8: Content of CD details view	7
Figure 9: Windows XP Content of CD	8
Figure 10: Certificate Import Wizard	9
Figure 11: File to import	10
Figure 12: Certificate Import Wizard: Password	11
Figure 13: Certificate Import Wizard: Setting certificate location	12
Figure 14: Certificate Import Wizard: Completing the Certificate Import Wizard	13
Figure 15: Certificate Import Wizard: Import successful	13
Figure 16: Certificate Import Wizard	15
Figure 17: File to import	16
Figure 18: Certificate Import Wizard: Entering Password	17
Figure 19: Enter Password	17
Figure 20: Certificate Store location	18
Figure 21: Complete install screen dump	19
Figure 22: Certificate Import Wizard: Import successful	19

Introduction

This guide demonstrates how to install a location certificate that will not prompt for a password each time a log in is attempted, enabling access to limited functions within the Medicare Australia, Health Professional Online Services (HPOS).

The following instructions will work with most Microsoft Windows 32 bit XP installs.

If you experience any problems, please call the eBusiness Service Centre on **1800 700 199****.

Location Certificate install

Important: If a password prompt is preferred for each log in to HPOS, please follow the user guide for *Installing a Location Certificate with a Password prompt to enable access to HPOS (XP)*.

To install the location certificate you will require local administrator access to your computer. If you do not have administrator access, please discuss this with your system administrator.

Step 1

Insert the CD you have received from eCertificates, into your CD/DVD drive.

The following screen will display.



Figure 1: Index html page

Close the above screen as this relates to installations allowing online claiming.

Go to *Step 2*.

Step 2

Click *Start* at the bottom left of the screen and select *Run*.

The following screen will display.

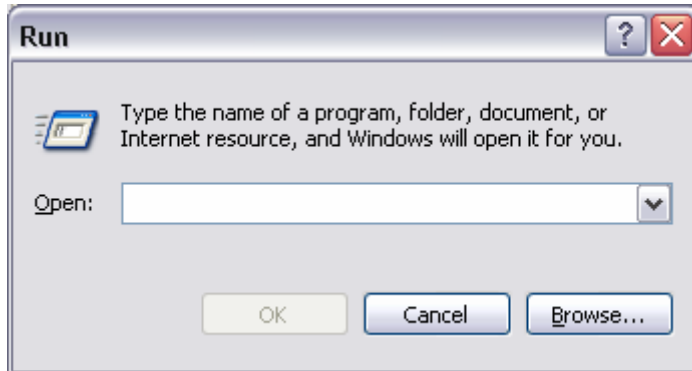


Figure 2: Run

Type in 'explorer' and click *OK*.

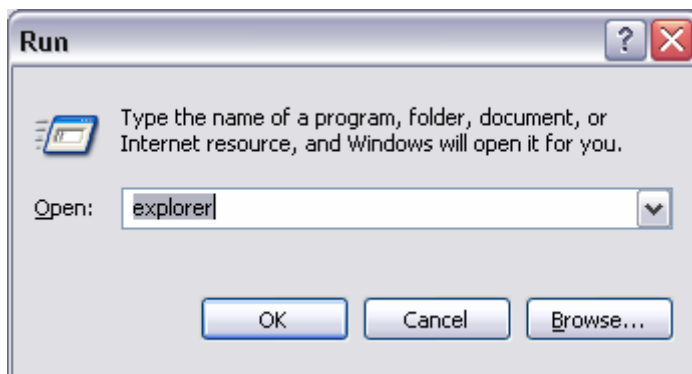


Figure 3: Run explorer

Step 3

Click *My Computer* as shown in the following screenshot.

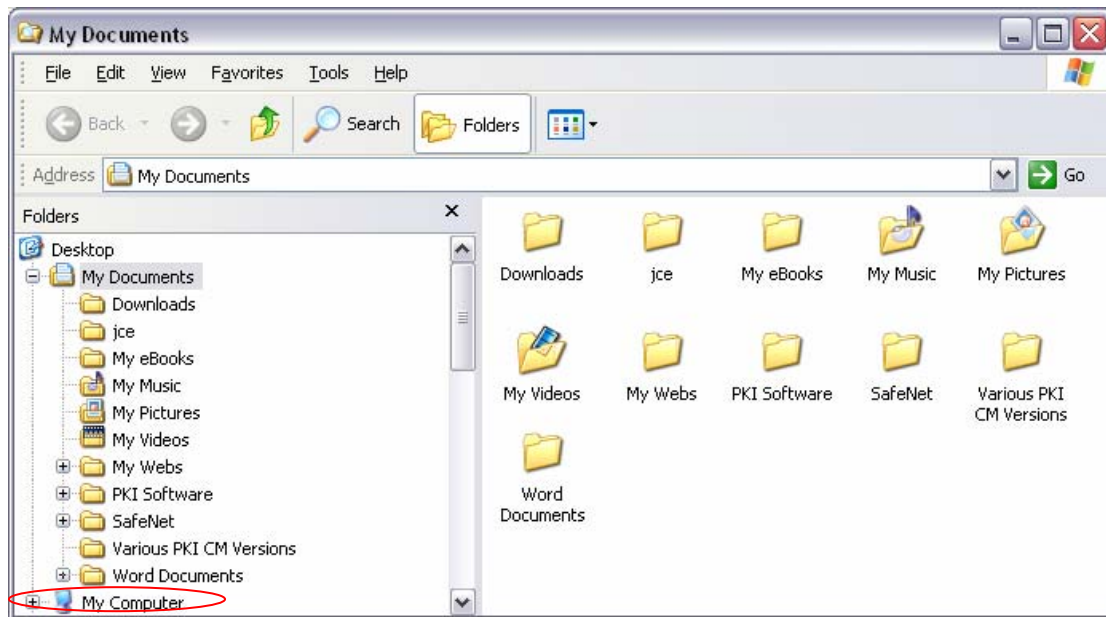


Figure 4: My Computer

The following screen will display.

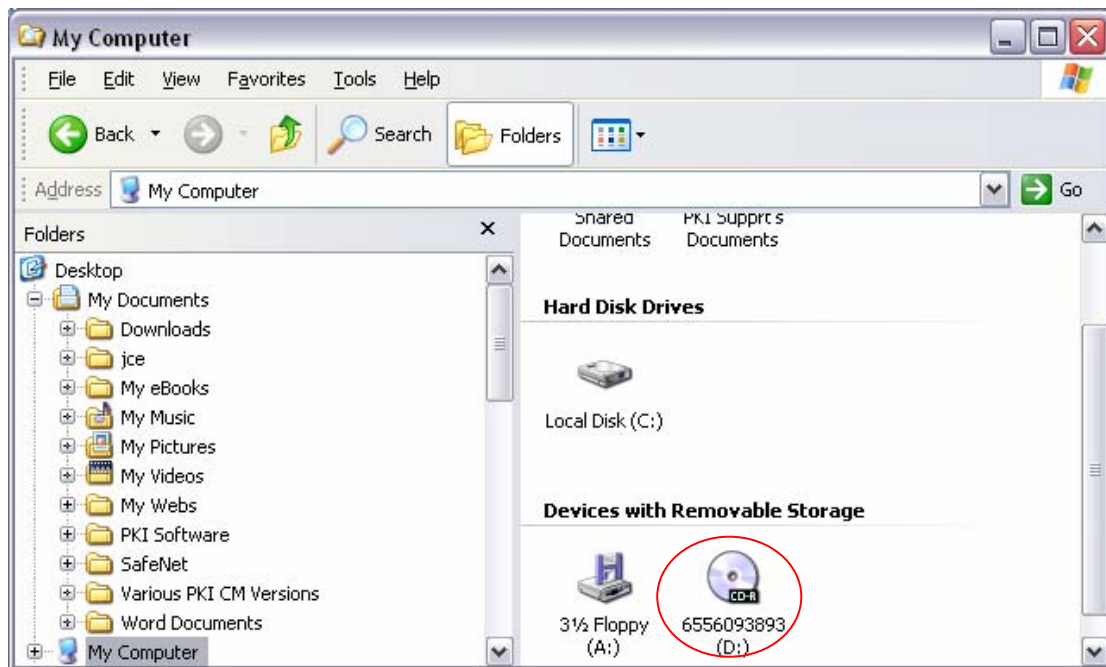


Figure 5: Windows Explorer CD Drive

Double click the CD/DVD drive as shown in the above screenshot.

Step 4

The following screen will display.

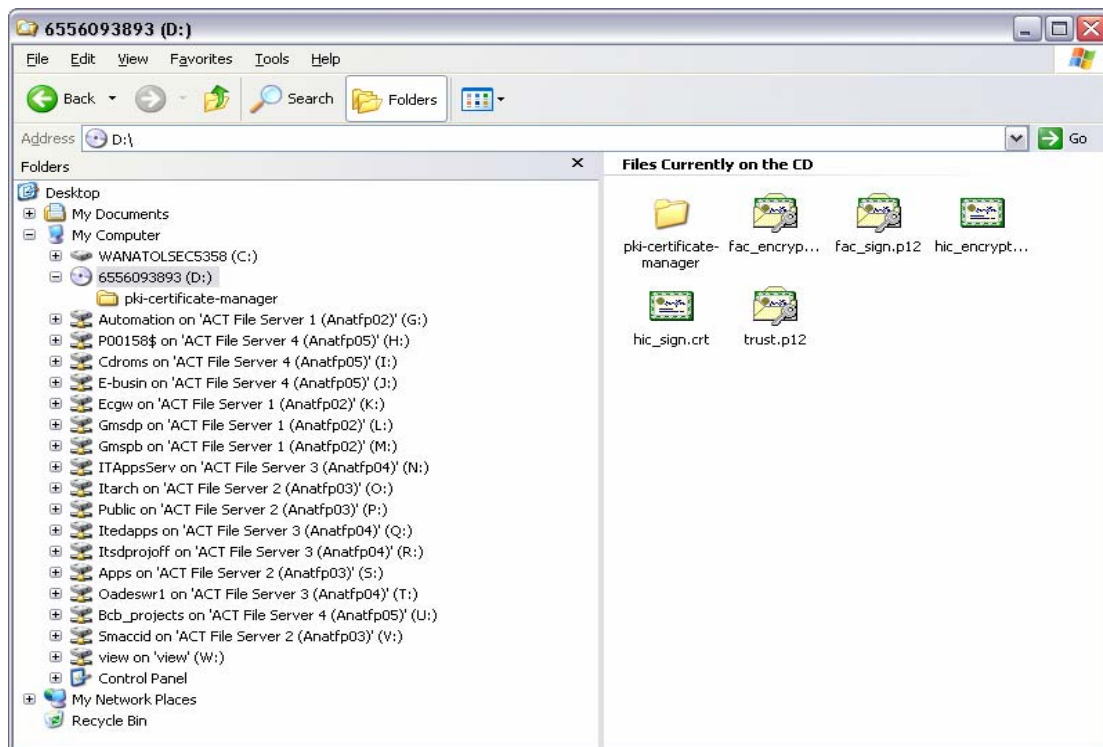


Figure 6: CD Content icon view

In order to see the full file names involved, switch the view to *Details* as shown in the following screenshot.

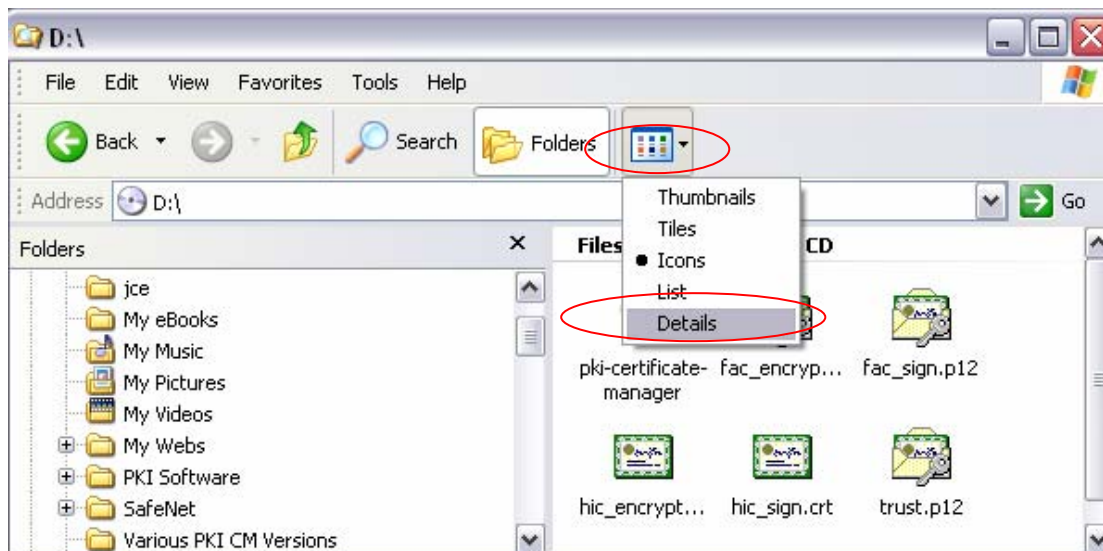


Figure 7: Changing to details view

The following screen will display.

Details view

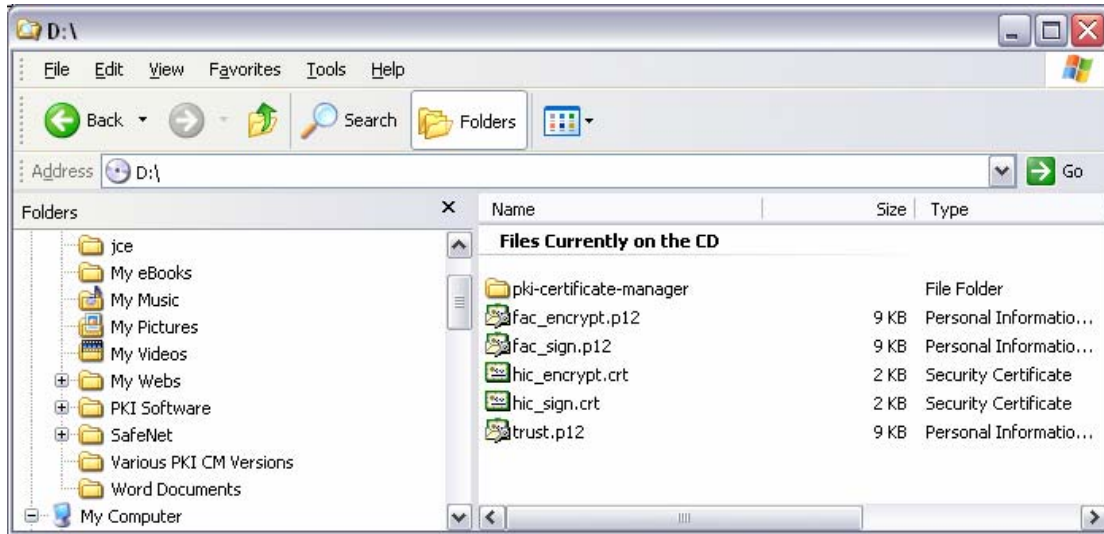


Figure 8: Content of CD details view

Step 5

You will need to install two files. These are the encryption certificate and the signing certificate.

- *fac_encrypt.p12*
- *fac_sign.p12*.

Double click the *fac_encrypt.p12* file as shown in the following screen.

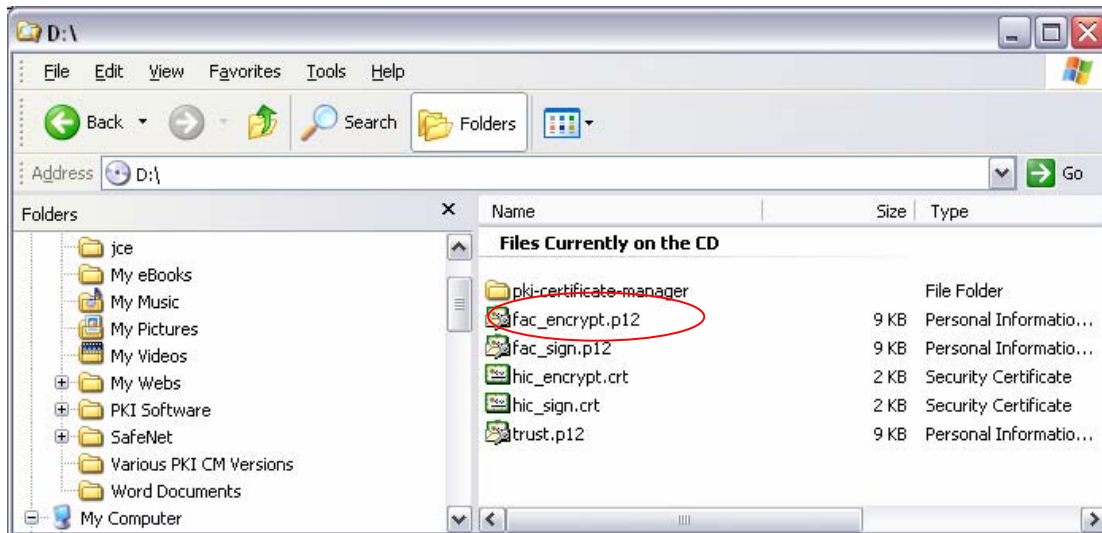


Figure 9: Windows XP Content of CD

Step 6

A Wizard will display.



Figure 10: Certificate Import Wizard

To continue click *Next*.

Step 7

The path of the certificate is displayed in the next screen.

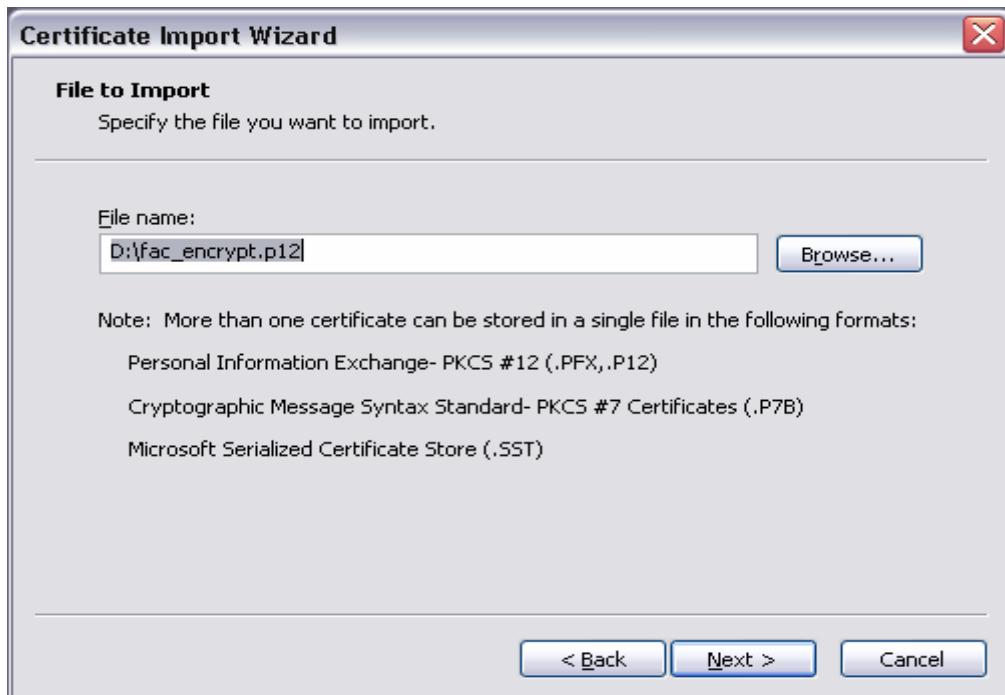


Figure 11: File to import

To continue click *Next*.

Step 8



Figure 12: Certificate Import Wizard: Password

Enter the password supplied with your new certificate, key in the *(PIC) passphrase*.

To continue click *Next*.

Step 9

The following screen will display.



Figure 13: Certificate Import Wizard: Setting certificate location

Leave the settings as they are displayed in Figure 13.

To continue click *Next*.

Step 10

The following screen will display.

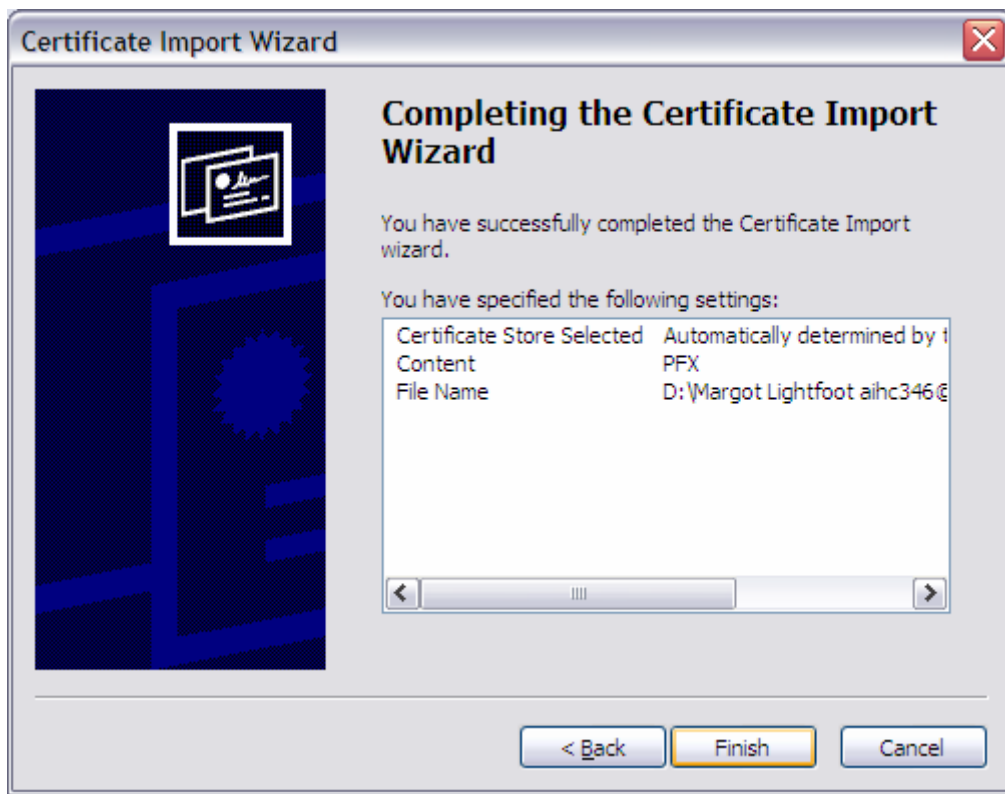


Figure 14: Certificate Import Wizard: Completing the Certificate Import Wizard

To continue click *Finish*.

The following message will display.

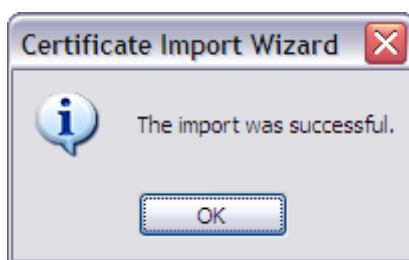


Figure 15: Certificate Import Wizard: Import successful

Click *OK* to finish.

Step 11

Repeat Steps 5 to 10 for the signing certificate

- *fac_sign.p12*.

Once both files have been installed go to *step 12*.

Step 12

You will now need to ensure you have the correct Chain of Trust installed for the Medicare Australia issued certificates.

Double click *trust.p12* from the CD as shown in *step 5*.

A Wizard will display.



Figure 16: Certificate Import Wizard

To continue click *Next*.

Step 13

The path of the certificate will be displayed in the next screen.



Figure 17: File to import

To continue click *Next*.

Step 14

The following screen will display.



Figure 18: Certificate Import Wizard: Entering Password

Important: key in the following password 'Pass-123' (the 'P' is in upper case).

See Figure 4 below.

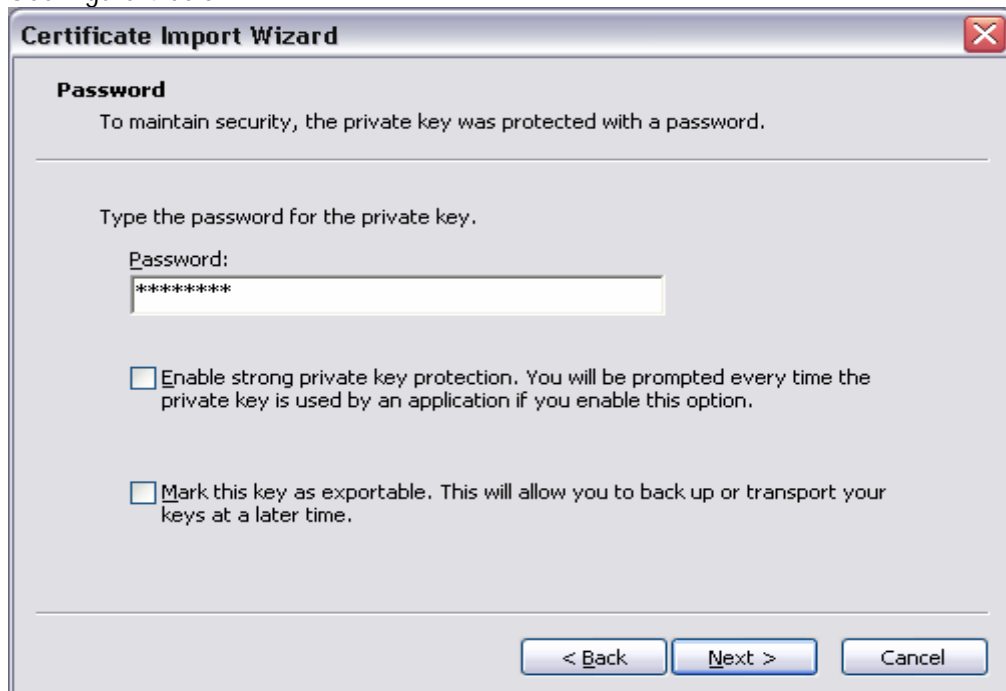


Figure 19: Enter Password

To continue click *Next*.

Step 15

The following screen will display.

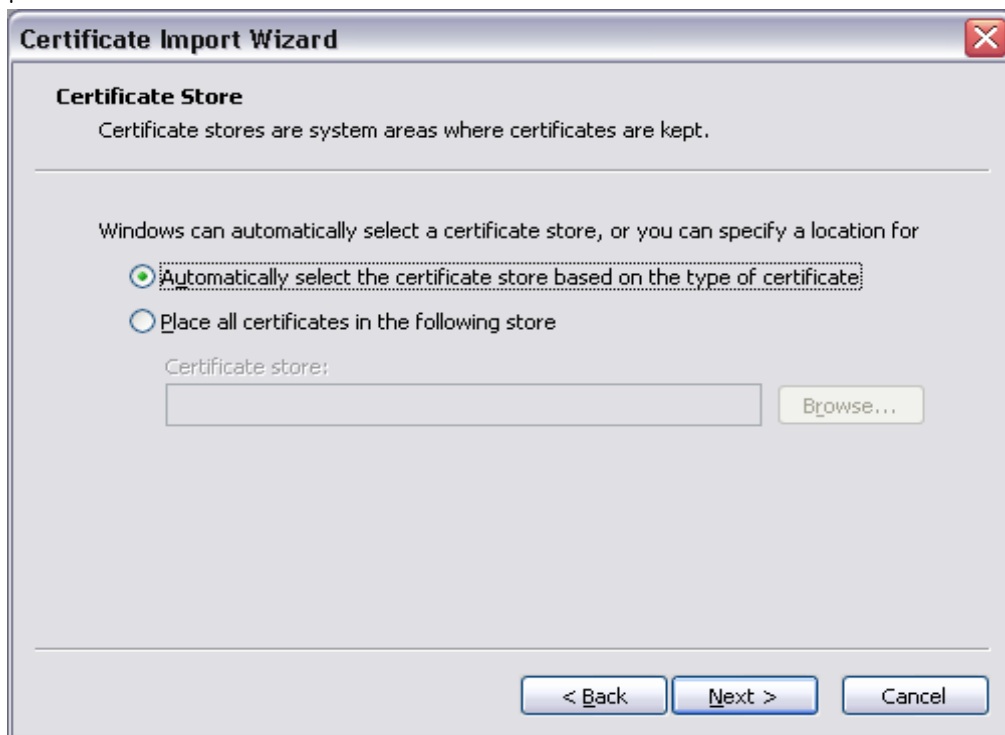


Figure 20: Certificate Store location

To continue click *Next*.

Step 16

The following screen will display.

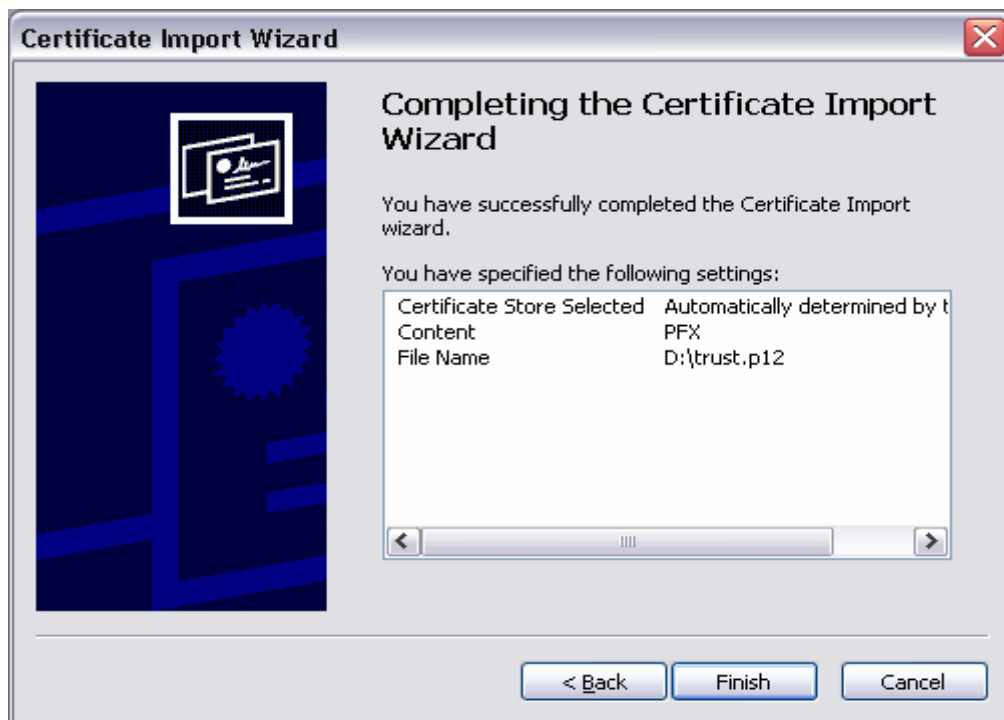


Figure 21: Complete install screen dump

To continue click *Finish*.

The following message will display.

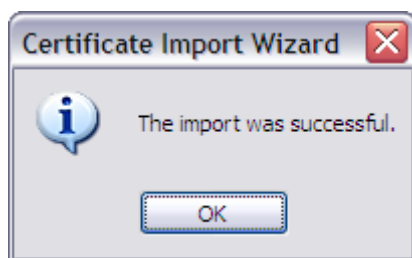


Figure 22: Certificate Import Wizard: Import successful

Click *OK* to complete the installation.

You have successfully completed installing all components of the location certificate.

Important: each computer that needs to access the HPOS page will need the certificate installed on that local machine.

If you continue to experience problems you can refer to our *Trouble Shooting Guide* or contact our eBusiness service centre on **1800 700 199**** for further assistance

** Call charges apply from mobile and pay phones only,