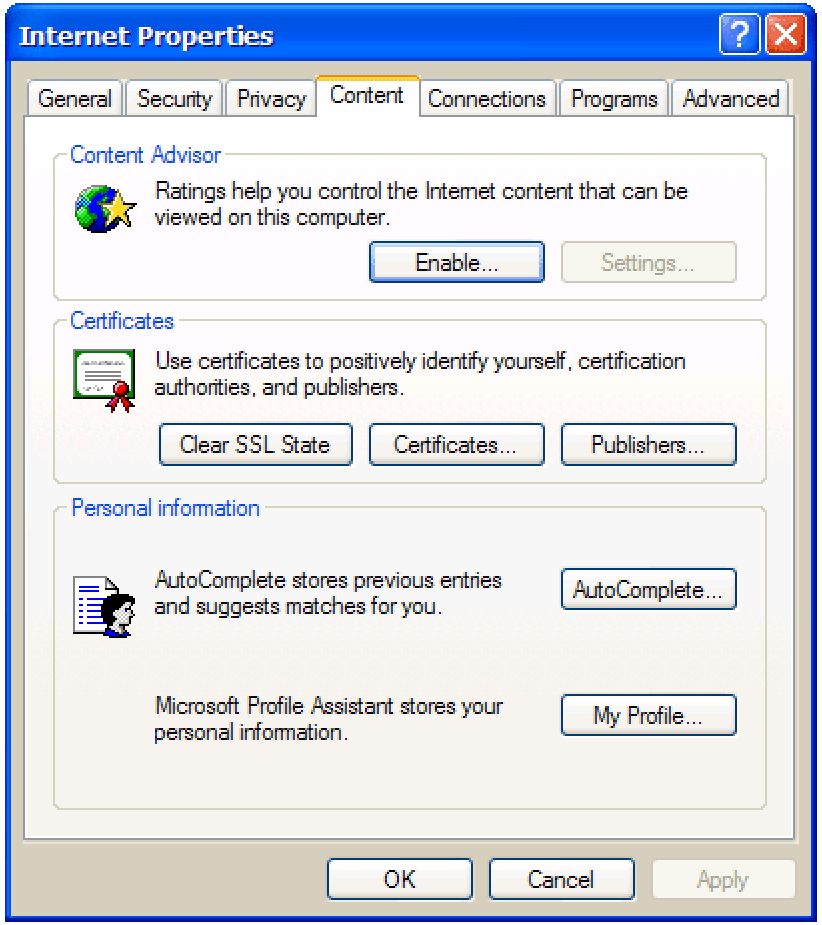
How to Export a Digital Certificate

The purpose of exporting a Digital Certificate is two-fold: first to enable it to be installed so that **Export-It** may use it and also to place it in a known location for later use. It is very important that a Digital Certificate not be "lost" as there can be a significant charge to re-issue a certificate.

The process begins by invoking the "**Internet Properties**" dialog. This can be done from **Internet Explorer** by selecting "**Internet Options…**" from the "**Tools**" menu or by pressing the Taskbar "***Start***" button and running the "**Internet Options**" applet from "**Control Panel**" settings. When the "**Internet Properties**" dialog appears, click on the "**Content**" tab.



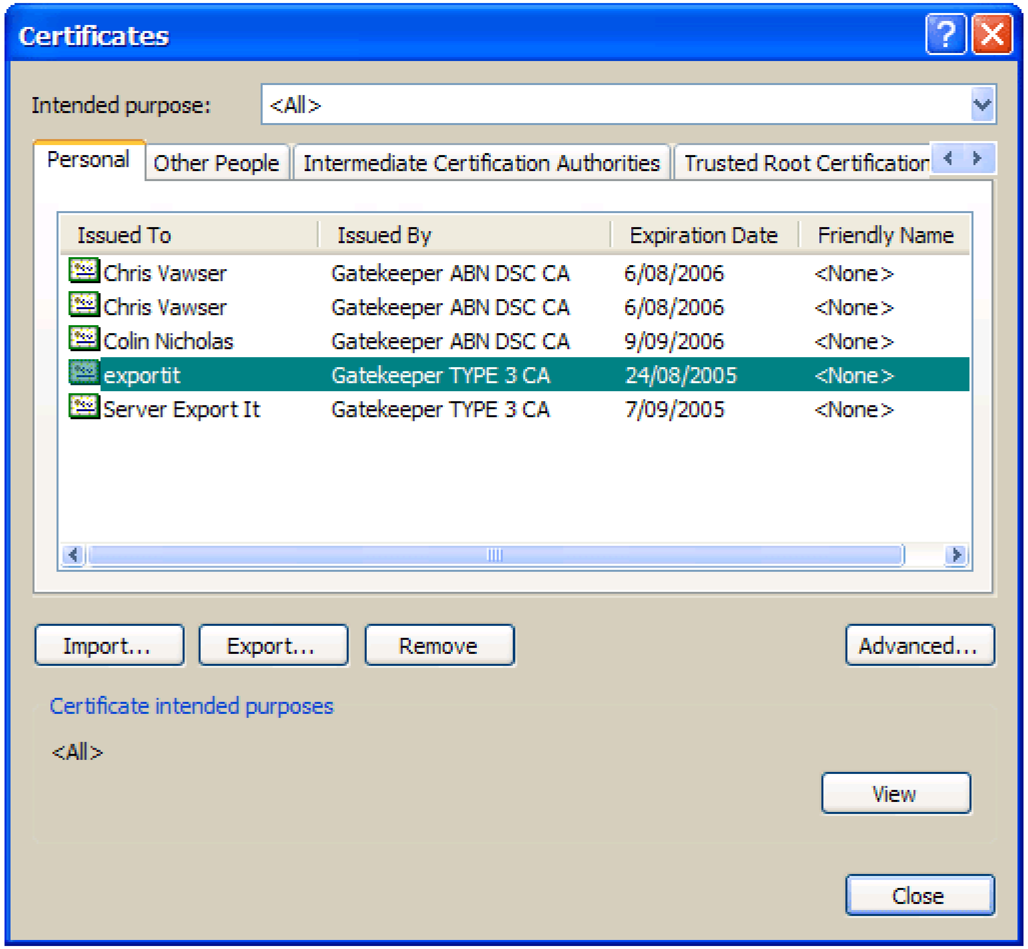
Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

Press the "**Certificates…**" button [above] to open the "**Certificates**" dialog.


Certificates
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

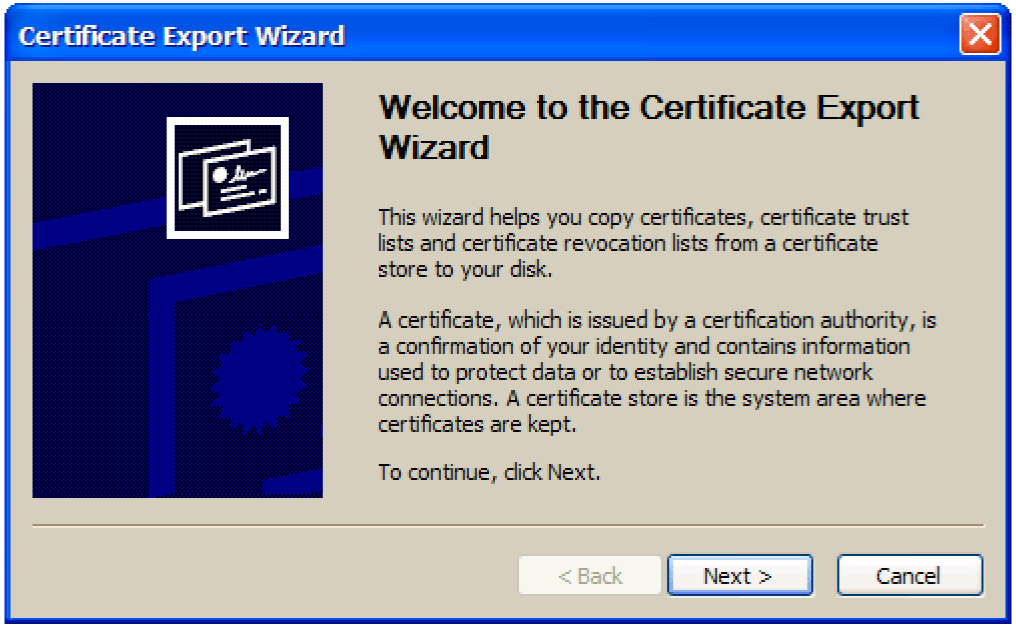
Intended purpose: <All>

Issued To	Issued By	Expiration Date	Friendly Name
Chris Vawser	Gatekeeper ABN DSC CA	6/08/2006	<None>
Chris Vawser	Gatekeeper ABN DSC CA	6/08/2006	<None>
Colin Nicholas	Gatekeeper ABN DSC CA	9/09/2006	<None>
exportit	Gatekeeper TYPE 3 CA	24/08/2005	<None>
Server Export It	Gatekeeper TYPE 3 CA	7/09/2005	<None>

<All>

In the "**Certificates**" dialog click on the site's Digital Certificate so that it is highlighted. Note that the certificate may be a "**Gatekeeper TYPE 3 CA**" (called an "equipment" certificate) or a "**Gatekeeper ABN DSC CA**" (a "non-individual" Type 2 certificate) that has a "Key Usage" including "**Non-repudiation**". In the case of a "**Gatekeeper ABN DSC CA**" ("non-individual" Type 2) it is strongly recommended that the "**View**" button be pressed and the "Key Usage" details be checked to verify that "**Non-repudiation**" is included. This is the only way to be certain that a Type 2 certificate will be acceptable to Australian Customs for use with CMR-ICS.

When the site's certificate is selected [highlighted], and verified if it is a "**Gatekeeper ABN DSC CA**", then press the "**Export…**" button to invoke the "**Certificate Export Wizard**" [see next page].



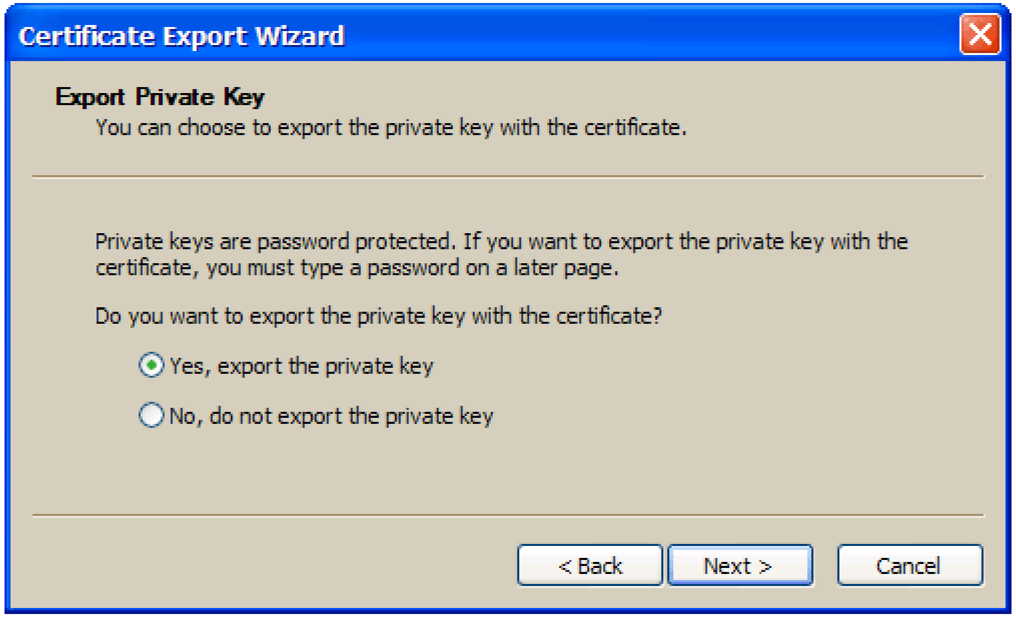
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

On the “**Welcome**” page press the “**Next >**” button.



Export Private Key
You can choose to export the private key with the certificate.

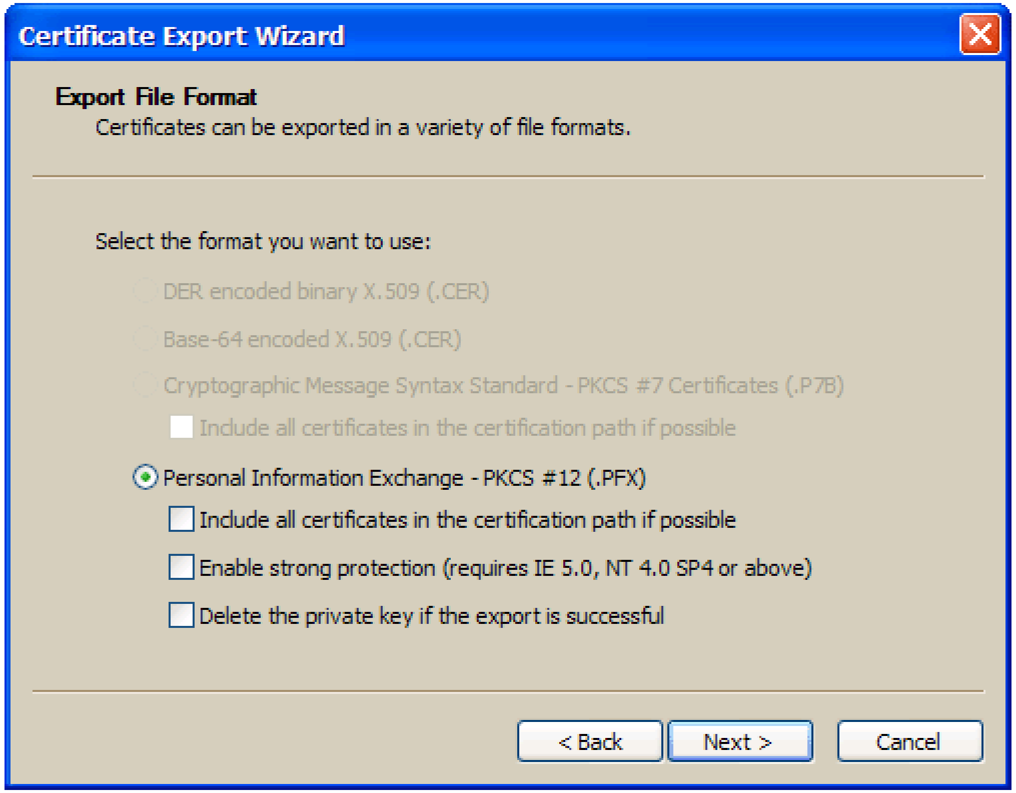
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

On the “**Export Private Key**” page tick “Yes, export the private key” *(the private key is needed to create Secure EDI messages for CMR-ICS)* and then press the “**Next >**” button.



Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

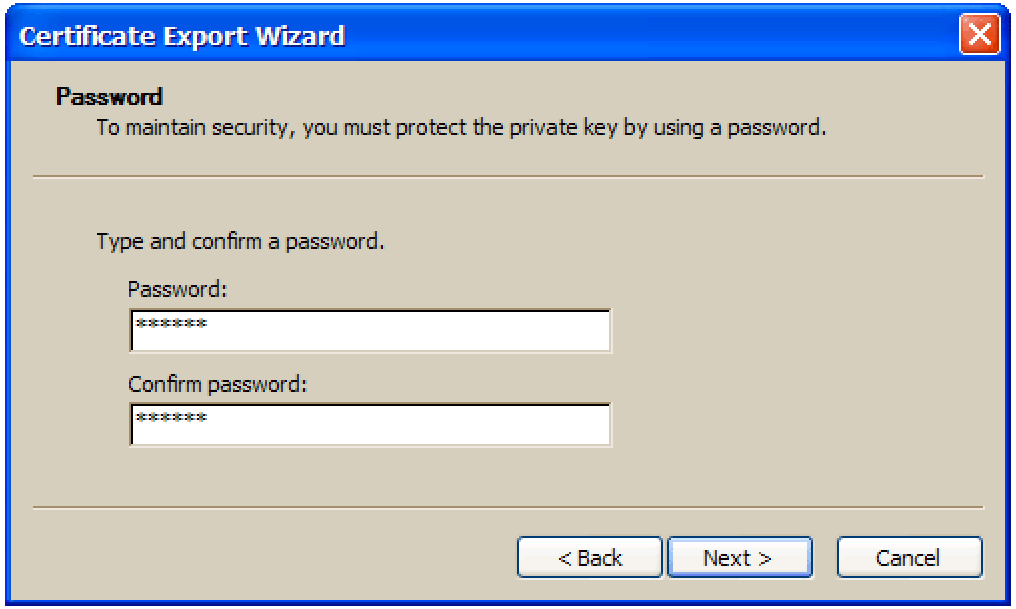
□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

On the “**Export File Format**” page select “Personal Information Exchange - PKCS #12 (.PFX)” format *and make absolutely certain that* *__none__* *of the checkboxes below it are selected!* If any of these checkboxes are ticked then there will be problems. For example, if “Enable strong protection…” were left with a tick then every time that **Export-It** uses the certificate an annoying dialog would have to be answered before encryption or decryption of messages could occur.

When the “**Export File Format**” page looks like the sample above press the “**Next >**” button to go to the next step.

WARNING: If the “Personal Information Exchange - PKCS #12 (.PFX)” option is not available (i.e. is greyed-out) *then the certificate selected does not contain a private key and is not usable for Secure EDI messages!* Either search other tabs in the “**Certificates**” dialog for other versions of the certificate and try them or arrange with VeriSign to download the certificate again. The exported certificate __must__ contain a private key and __must__ be in “(.PFX)” format.



Certificate Export Wizard

Password

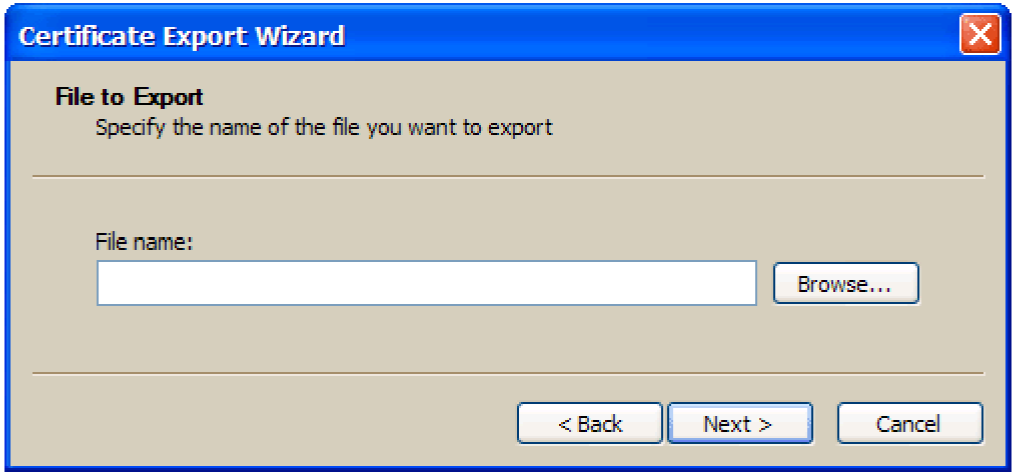
To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password: *******

Confirm password: *******

On the “**Password**” page enter the certificate password twice, first in the “Password” field and again in “Confirm Password” field. *Remember this password it must be used to access the certificate!* Then press the “**Next >**” button.



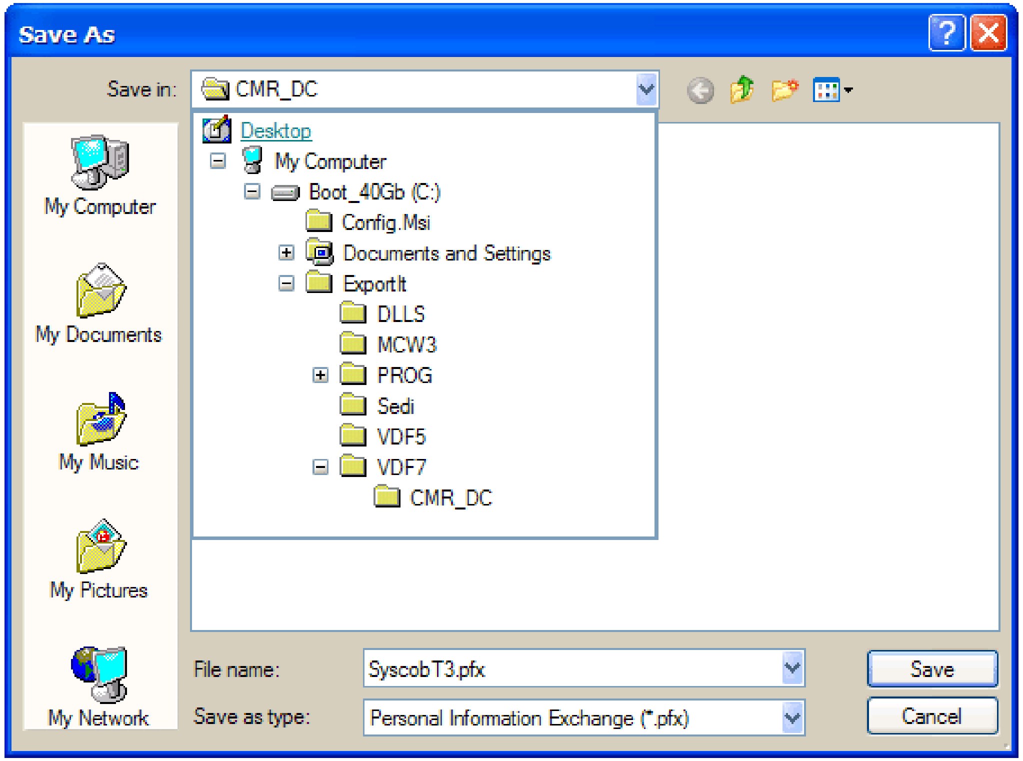
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

On the “**File to Export**” page press the “**Browse...**” button to open the “**Save As**” dialog seen in the upper-right. In the dialog navigate to the **CMR_DC** folder under the **VDF7** folder of the SEDI machine’s “local” drive.



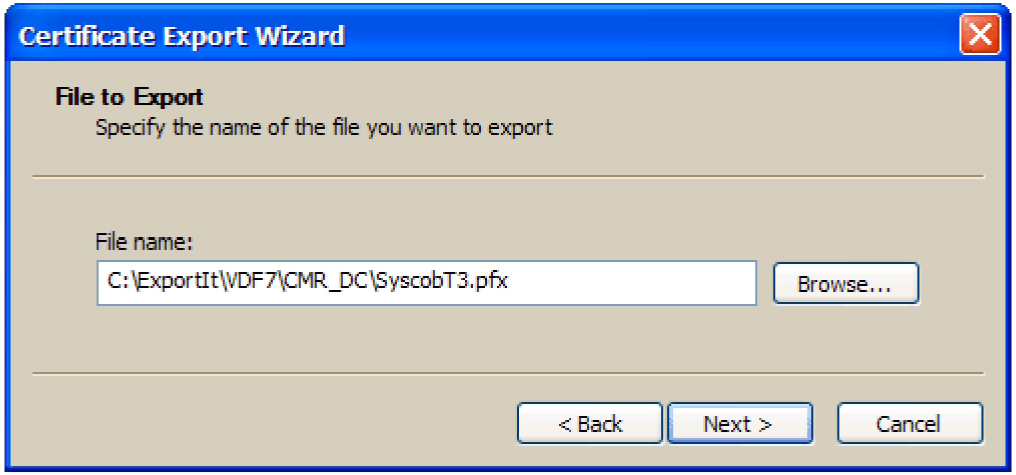
Save As

Save in: CMR_DC

File name: SyscobT3.pfx

Save as type: Personal Information Exchange (*.pfx)

Type a filename for the certificate in the “File name” box and then press the “**Save**” button. This should put the path and filename into the “**File to Export**” page, as in the example below. Then press the “**Next >**” button to finish exporting the certificate.

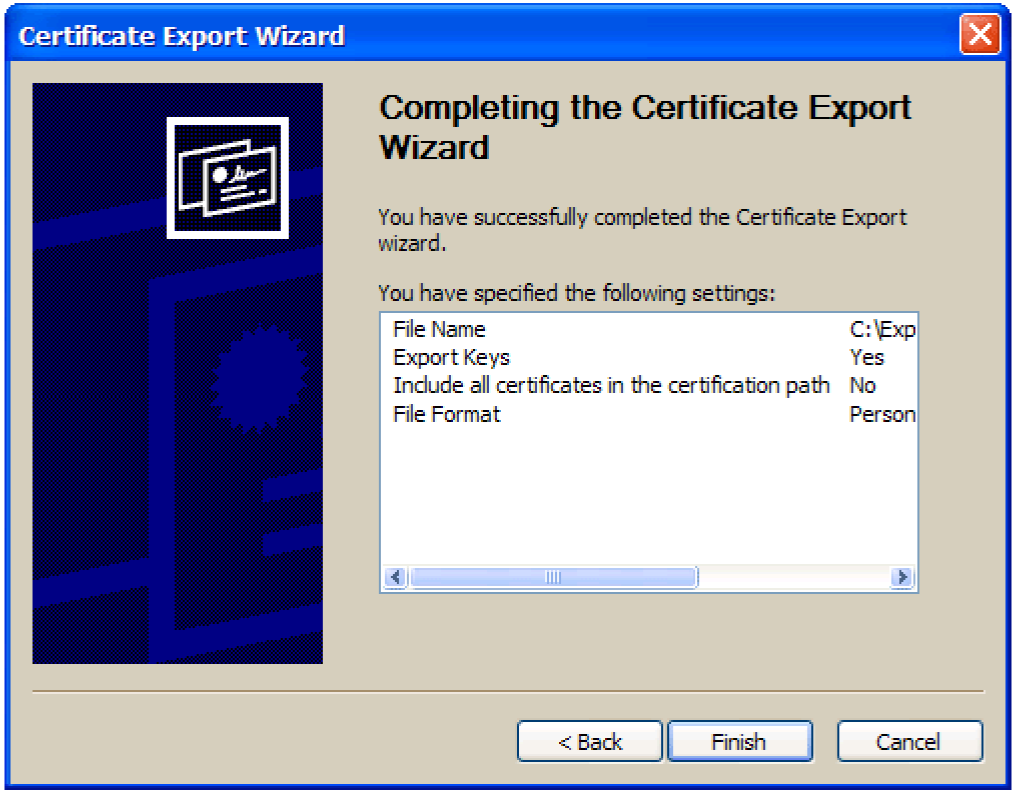


Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name: C:\ExportIt\VDF7\CMR_DC\SyscobT3.pfx



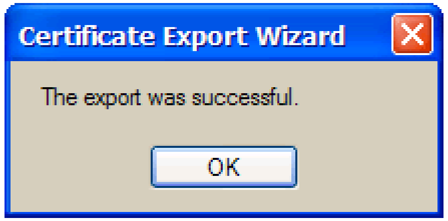
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Exp
Export Keys	Yes
Include all certificates in the certification path	No
File Format	Person

On the “**Completing the Certificate Export Wizard**” page review the settings, especially that “Export Keys” is “Yes”, and press the “**Finish**” button. This should write the certificate into a file that can be used by the **Export-It** system. If the certificate export is successful then the following dialog will appear.



The export was successful.

Press the “**OK**” button on this dialog to complete the wizard.

Press the “**OK**” button in the “**Internet Properties**” dialog to close it. This completes the process of exporting a Digital Certificate, but it will now need to be imported into the **Export-It Certificate Manager** utility. Refer to the **Export-It** setup instructions for how to install this, and the three Customs, certificates.