

PKCS #12 FILES

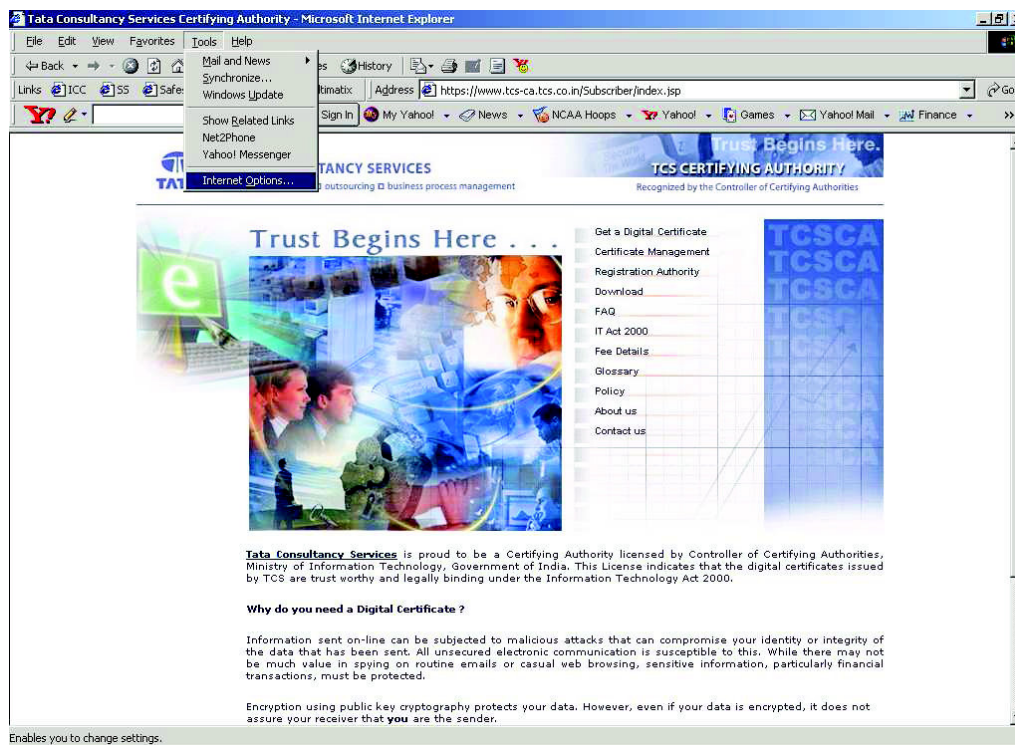
PKCS stands for Public Key Cryptographic Standard. PKCS #12 is the standard for transporting the private key along with the certificate securely. It has both the private key and the certificate. The private key is encrypted.

When the Subscriber downloads the certificate into the IE browser, the certificate is stored in the key store where the private key is generated. To use the credentials in some other machine, the Subscriber has to export the private key and the certificate from the browser as a PKCS #12 file.

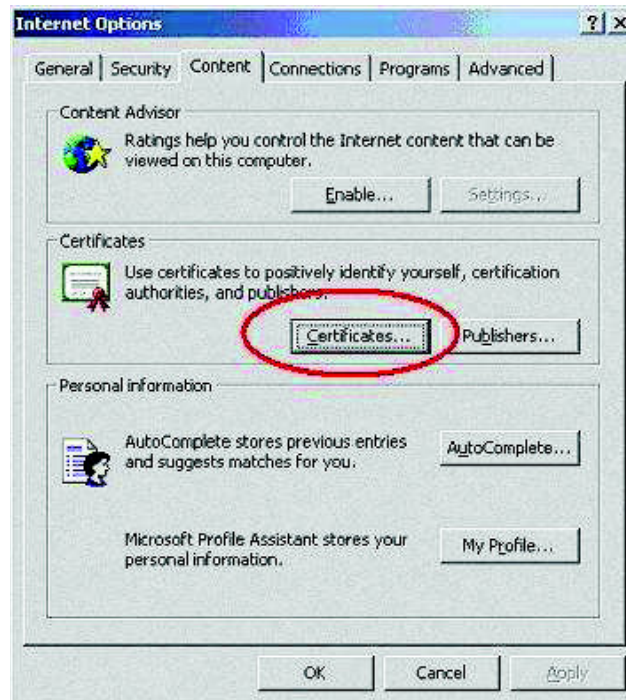
The extension for the PKCS #12 file is either “.p12” or “.pfx”

EXPORTING PKCS #12 FILE FROM THE BROWSER

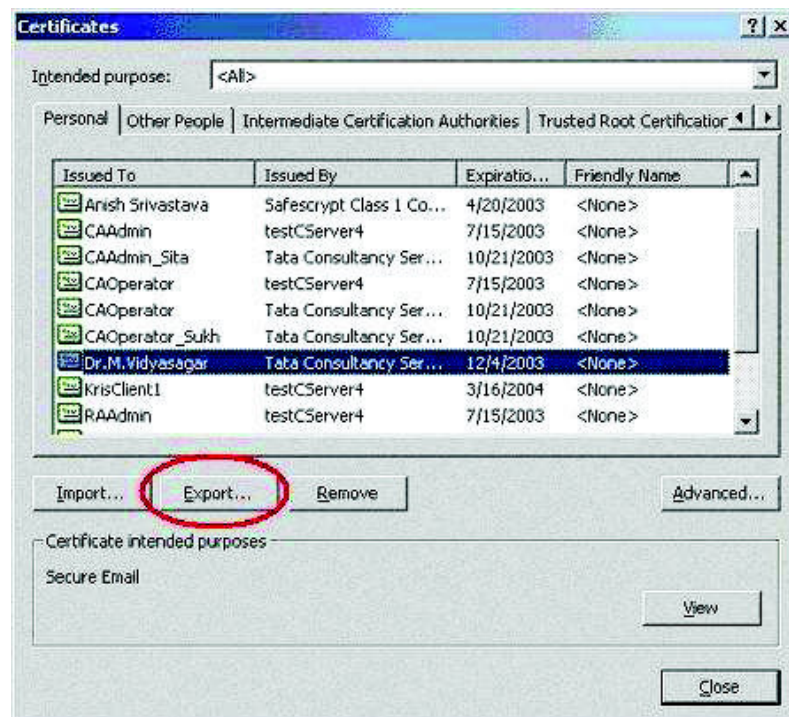
1. Click on the “Tools -> Internet Options” tab on the IE browser



- Click on the "Content -> Certificates" tab on the dialogue box shown.



- Choose the certificate to be exported and click on the export tab.



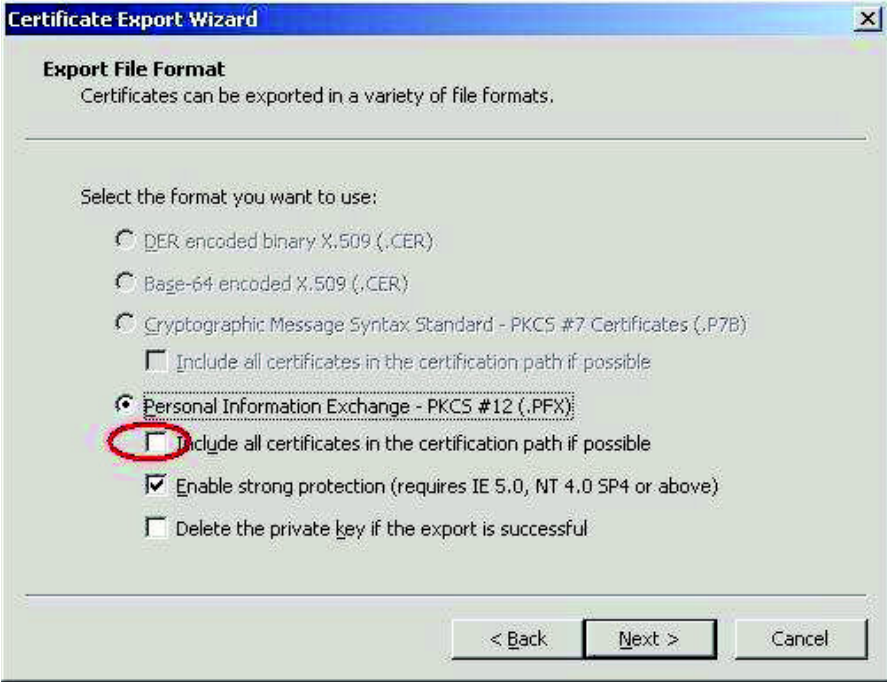
4. Click Next to the dialogue to continue



5. To export the private key with the certificate, choose the option "Yes" and click "Next"



6. Select the box indicated to include the CA certificate also with the Subscriber's certificate and Click "Next"



Certificate Export Wizard

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

< Back Next > Cancel

7. Enter the password to protect the PKCS#12 file



Certificate Export Wizard

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

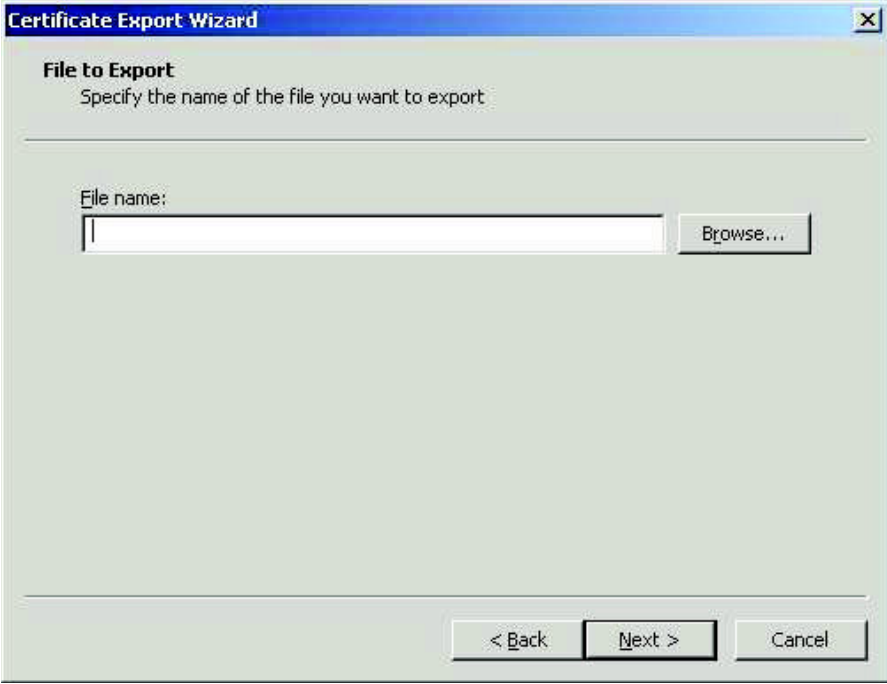
Type and confirm a password.

Password:

Confirm password:

< Back Next > Cancel

8. Choose the file name and location to save the file. Give the extension of the file as “.p12” or “.pfx”



The screenshot shows the 'File to Export' step of the Certificate Export Wizard. The window title is 'Certificate Export Wizard'. The main heading is 'File to Export' with the instruction 'Specify the name of the file you want to export'. Below this is a text box labeled 'File name:' with a 'Browse...' button to its right. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

9. Click Finish to export the private key and the certificates



The screenshot shows the 'Completing the Certificate Export Wizard' screen. The window title is 'Certificate Export Wizard'. On the left is a graphic of a certificate. The main heading is 'Completing the Certificate Export Wizard'. Below this is the text 'You have successfully completed the Certificate Export wizard.' followed by 'You have specified the following settings:'. A table lists the settings:

File Name	C:\Doc
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Person.

At the bottom of the window are three buttons: '< Back', 'Finish', and 'Cancel'.

10. A dialogue box will be shown for accessing the private key. Click “OK” to continue



11. A message will be shown indicating the successful completion of the export

