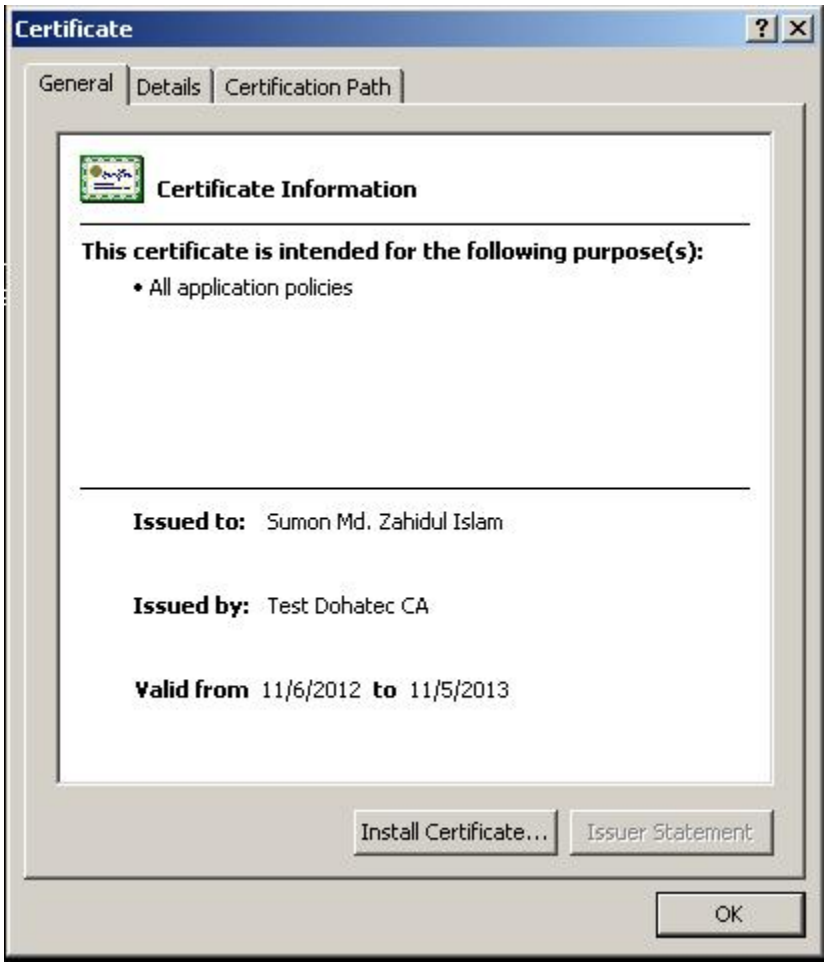
# Dohatec CA

## Certificate Export/Import

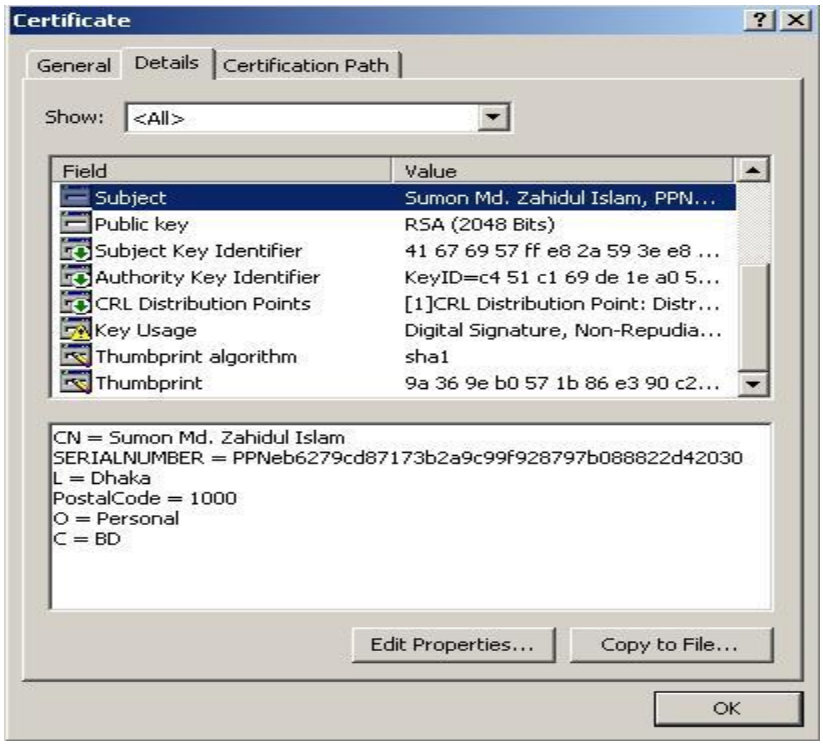
[VERSION 1.0]

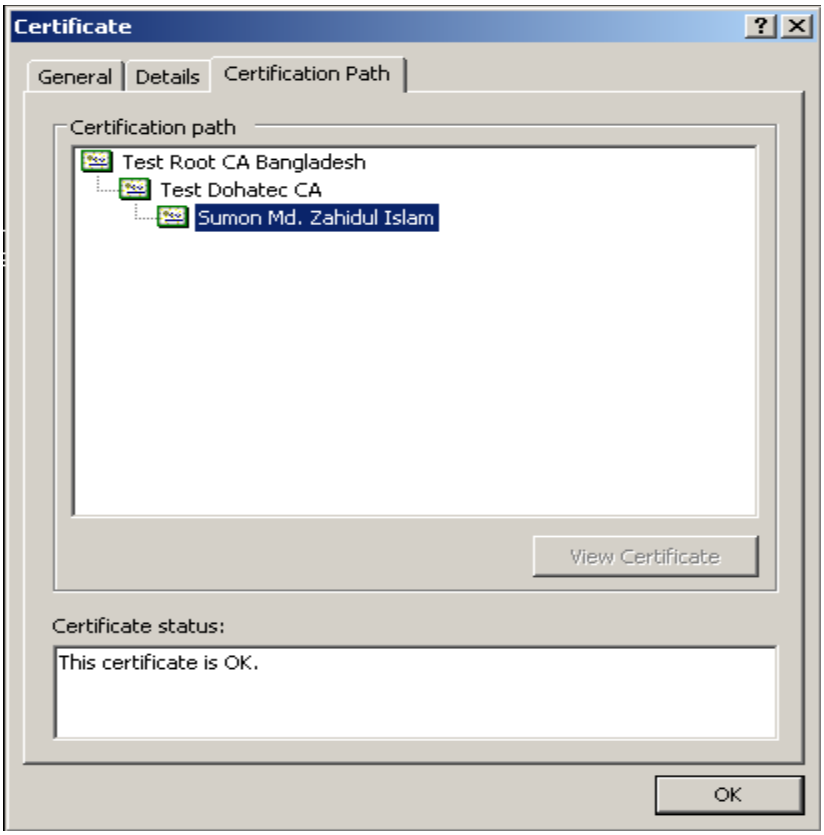
# 1 Digital Certificate

Certificates issued by Dohatec CA are in X.509 v3 format. In Microsoft windows machines, these are recognized by the extension '.cer'.
To view a certificate, simply double click the .cer file.




- To view the details of a certificate, click the 'Details' tab.


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
Sumon Md. Zahidul Islam, PPN...
Public key
RSA (2048 Bits)
Subject Key Identifier
41 67 69 57 ff e8 2a 59 3e e8 ...
Authority Key Identifier
KeyID=c4 51 c1 69 de 1e a0 5...
CRL Distribution Points
[1]CRL Distribution Point: Distr...
Key Usage
Digital Signature, Non-Repudia...
Thumbprint algorithm
sha1
Thumbprint
9a 36 9e b0 57 1b 86 e3 90 c2...
CN = Sumon Md. Zahidul Islam
SERIALNUMBER = PPNeb6279cd87173b2a9c99f928797b088822d42030
L = Dhaka
PostalCode = 1000
O = Personal
C = BD
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Certification path
Test Root CA Bangladesh
Test Dohatec CA
Sumon Md. Zahidul Islam
View Certificate
Certificate status:
This certificate is OK.
OK

- The hierarchy of trust for a certificate can be seen by clicking the 'Certification Path' tab. In this example, the certificate is issued by Dohatec CA, whose certificate is issued by CCA Bangladesh.

# 2 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.

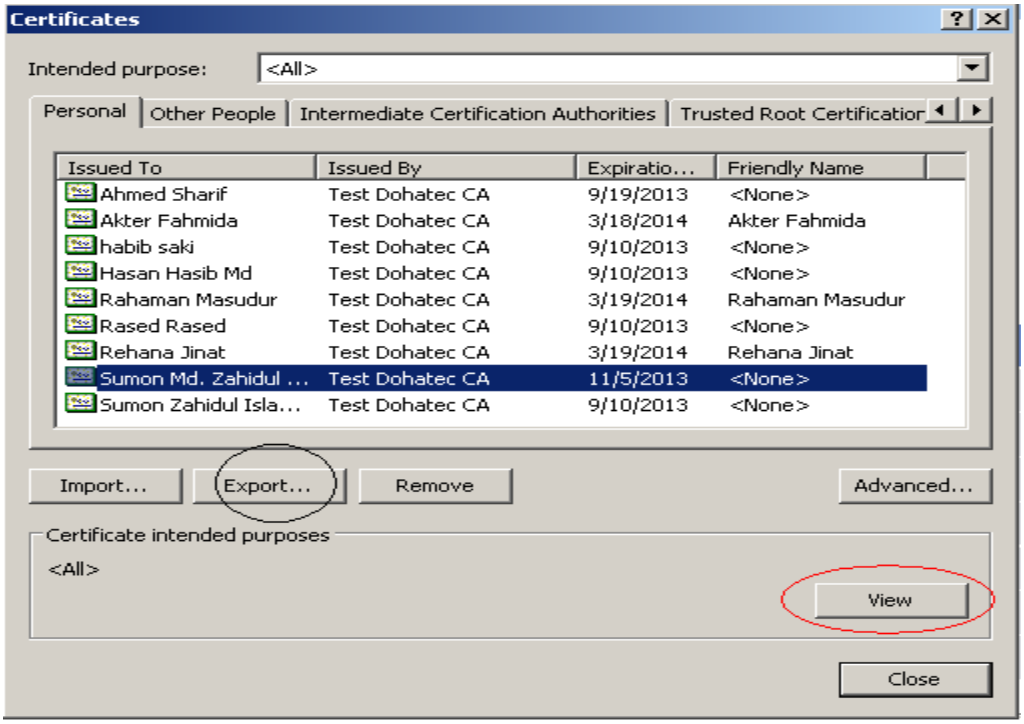
When the Subscriber downloads the certificate into the IE browser, the certificate is stored in the key store where the private key is generated. To use the credentials in some other machine, the Subscriber has to export the private key and the certificate from the browser as a PKCS #12 file.

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

## 2.1 Exporting a PKCS#12 File from the Browser

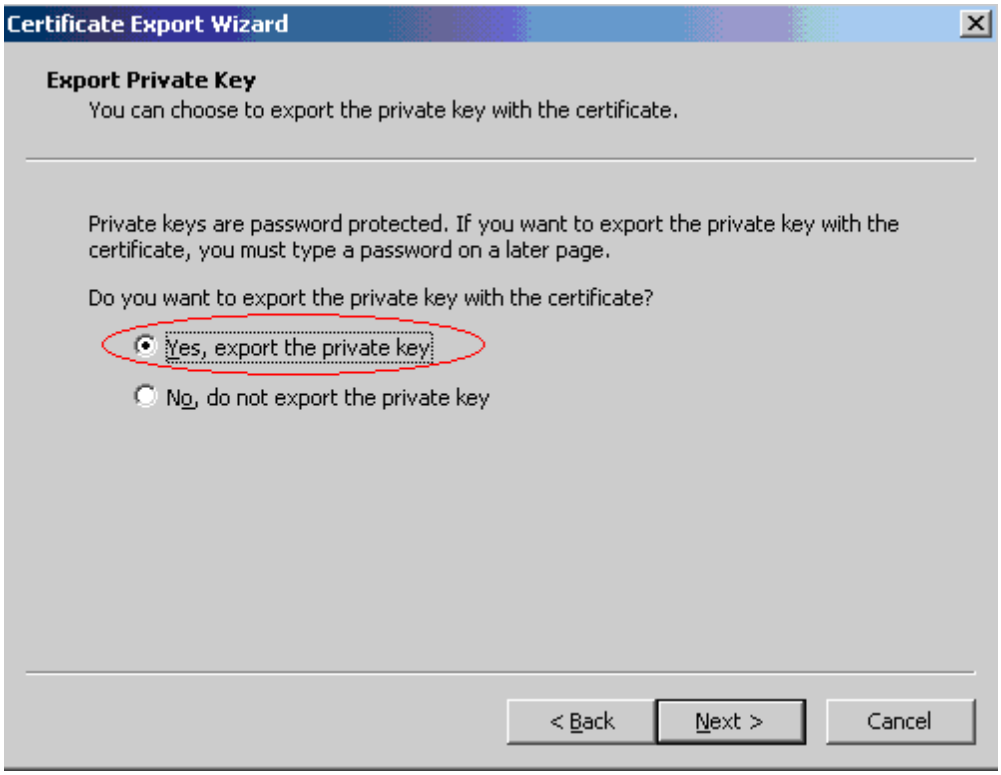
- Open an Internet browser window
- Click the Tools > Internet Options tab on the IE browser
- Click on the Content > Certificates tab on the dialog box shown.

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

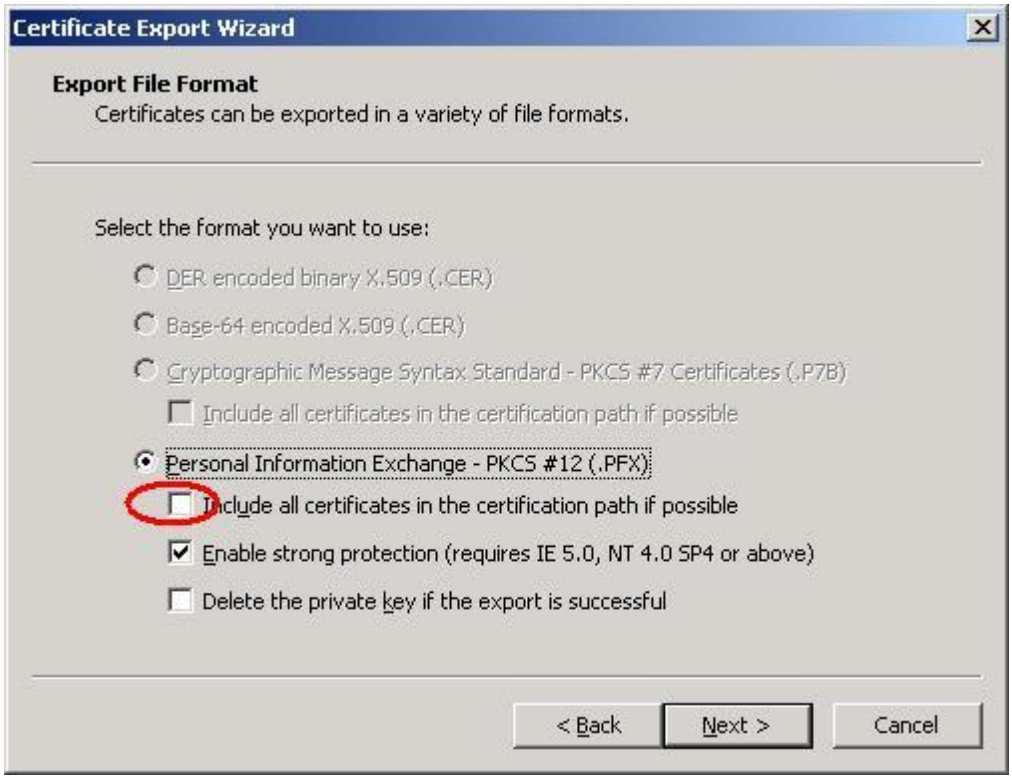



- Click Next to the dialog to continue.

- To export the private key with the certificate, choose the option 'Yes' and click 'Next'

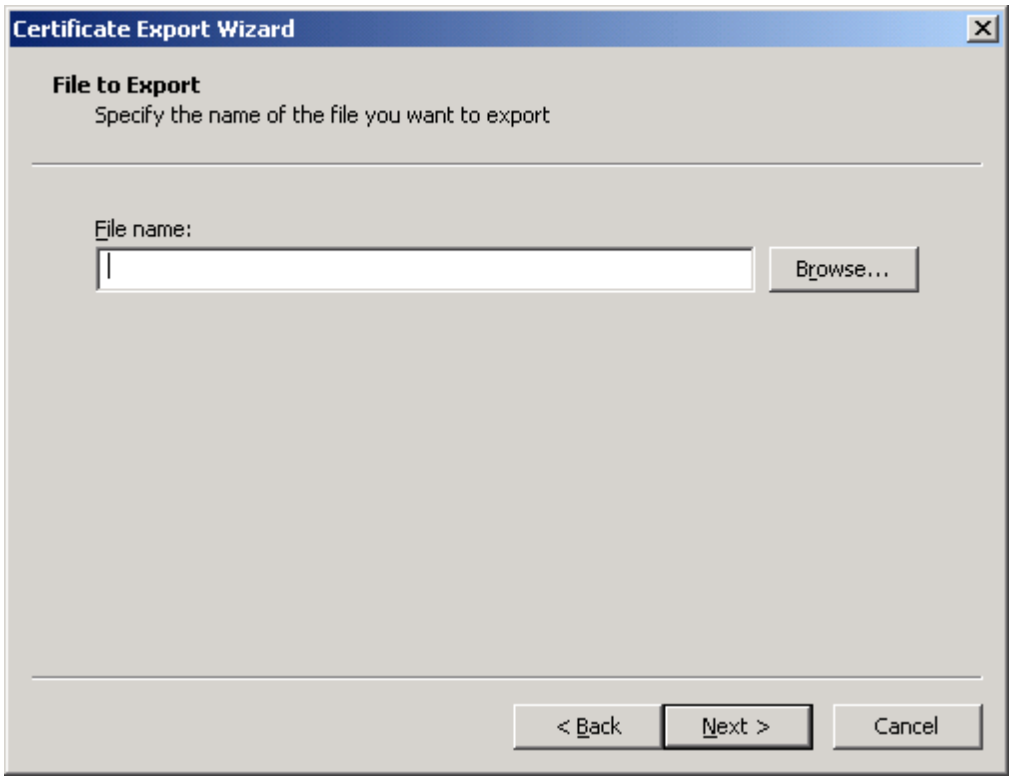



- Select the box indicated to include the CA certificate also with the Subscriber's certificate and Click 'Next'



- Enter the password to protect the PKCS#12 file


- Choose the file name and location to save the file. Give the extension of the file as '.p12' or '.pfx'



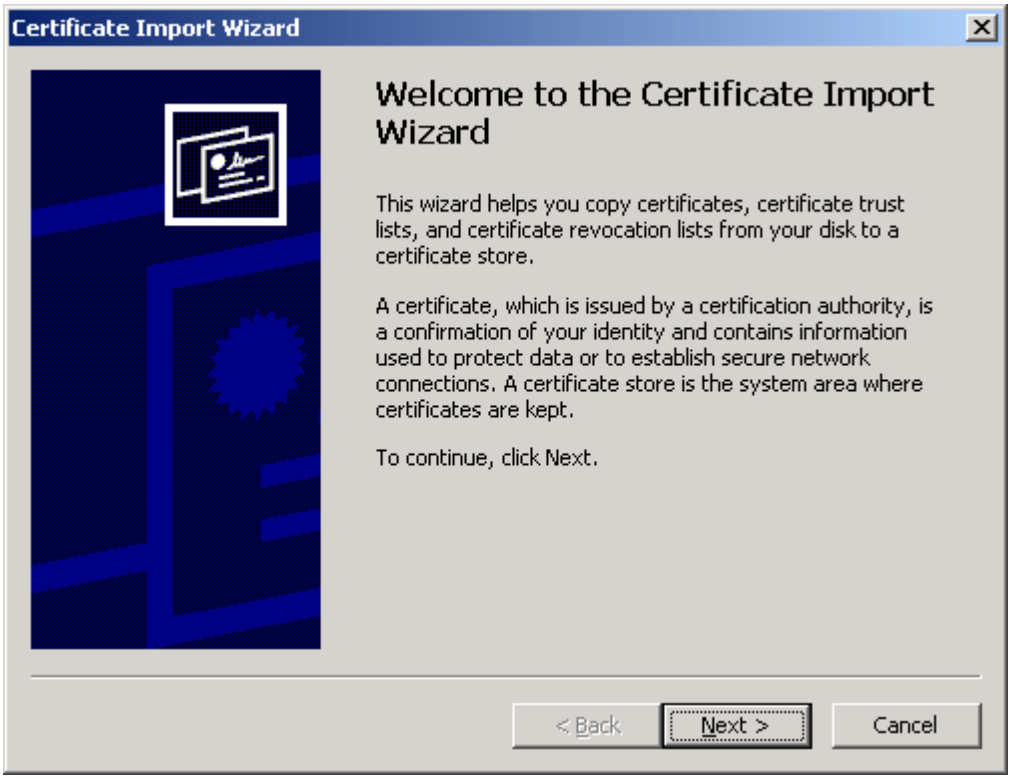
- Click Finish to export the private key and the certificates.


- A dialog box will be shown for accessing the private key. Click 'OK' to Continue

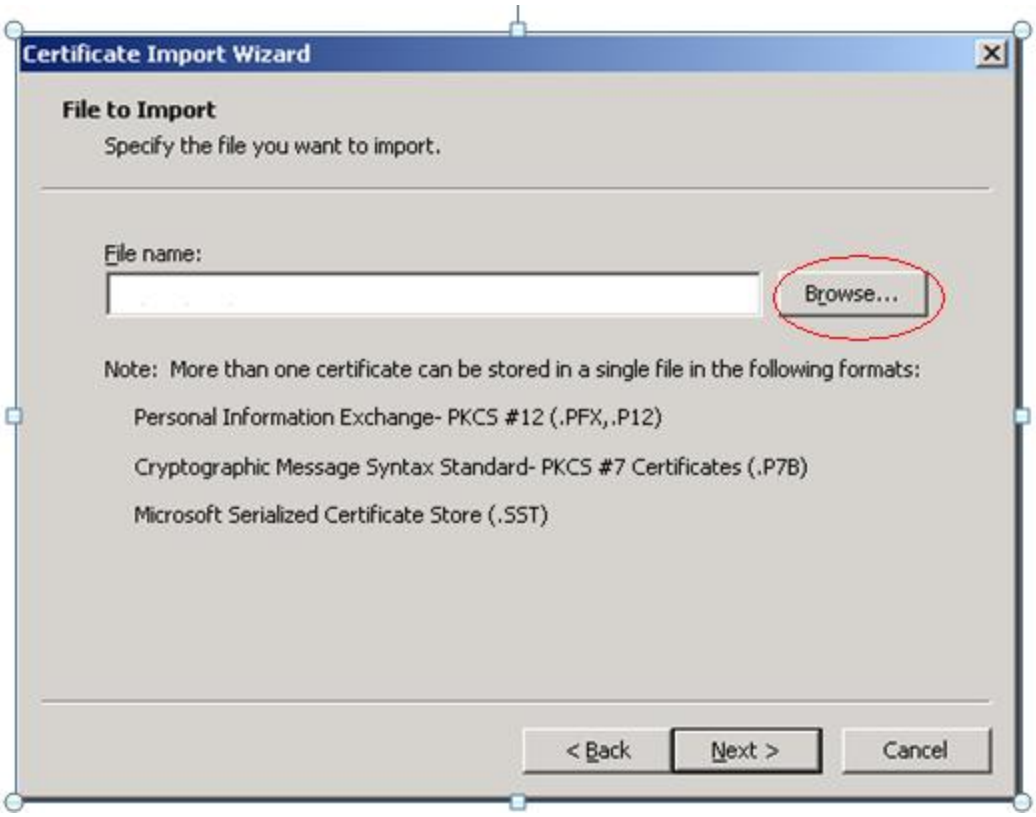

- A message will be shown indicating the successful completion of the export.


## 2.2 IMPORTING PKCS# 12 FILE INTO THE BROWSER

- Double-click on the '.p12' or '.pfx' file
- Click 'Next' on the dialog to continue.

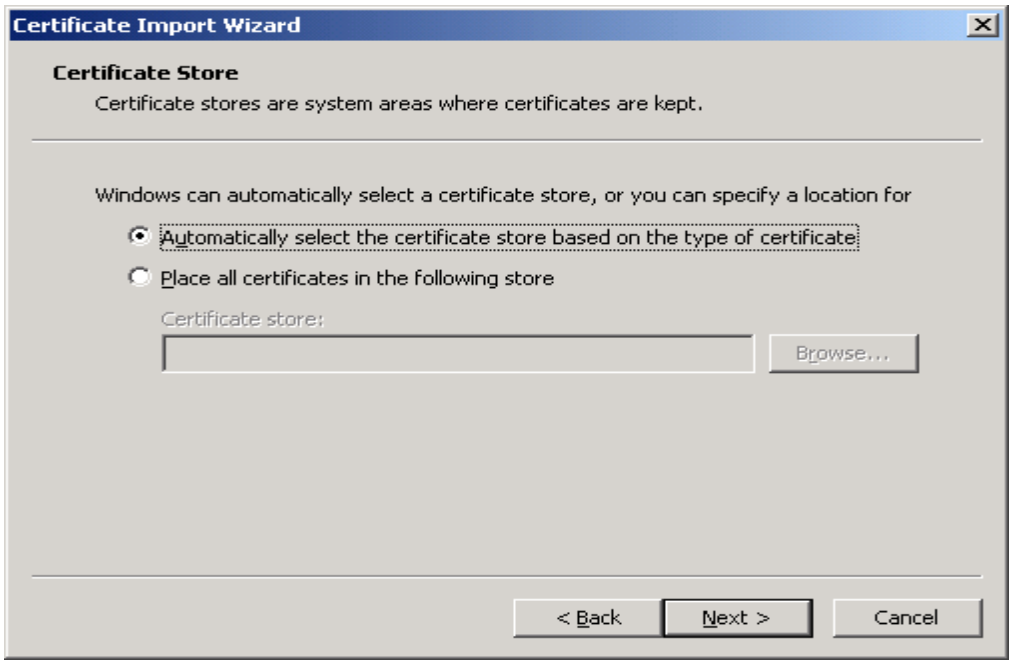



- Check the File location and click 'Next'.




- Enter the password, with which the private key is protected in the PKCS #12 file.

- Select the option 'Mark the private key as exportable', if you further want to export the private key from the browser. If it is not selected, then the private key cannot be exported from the browser again.
- Choose the option to automatically select the certificate store as shown and click 'Next'.




- Click 'Finish' to import the PKCS #12 file.

- Click ‘OK’ to import the private key.


- A message will be shown indicating the successful import of the private key.