CERTIFYING AUTHORITY

Exporting and Importing Certificates – A User Guide

CONTACT

TATA CONSULTANCY SERVICES
6TH FLOOR, 5-9-62, KHAN LATEEF KHAN ESTATE
FATEH MAIDAN ROAD, HYDERABAD - 500 001
TEL: +91 (40) 55671020 (D) / 5567000, EXT. - 1020
FAX: +91 (40) 55782930
WWW.TCS.COM / WWW.TCS-CA.TCS.CO.IN

Table of Contents

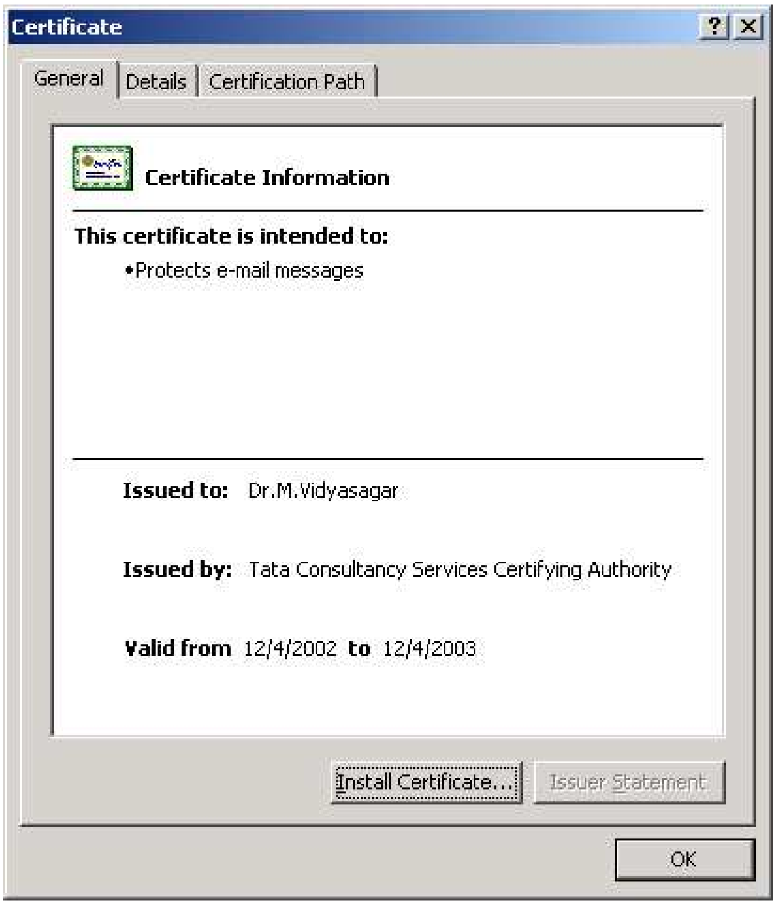
NOTICE OF PROPRIETARY INFORMATION

All information contained in or disclosed in this document, hereinafter called ‘Confidential Information’. By accepting this material, the recipient agrees that this Confidential Information will be held in confidence, and will not be reproduced, disclosed or used either in whole or in part, without prior permission from Tata Consultancy Services.

CERTIFICATES

The certificates issued by TCS-CA is in X509 v3 format. In Microsoft windows machines, it will be recognized by the extension “.cer”.

To view the certificates, double click the .cer file



Certificate Information

This certificate is intended to:

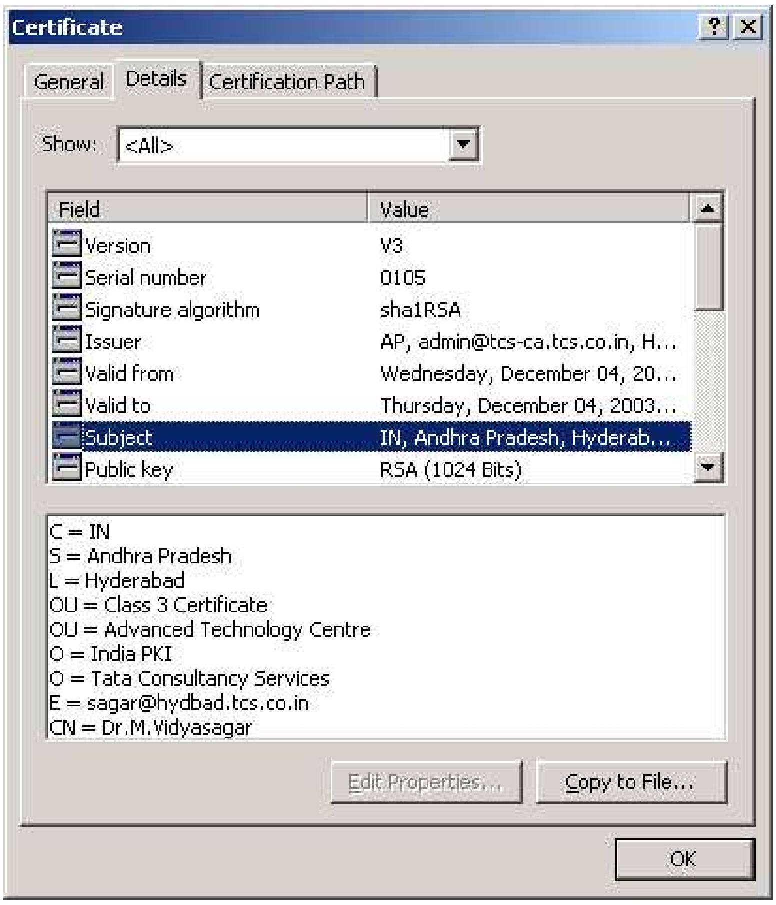
•Protects e-mail messages

Issued to: Dr.M.Vidyasagar

Issued by: Tata Consultancy Services Certifying Authority

Valid from 12/4/2002 to 12/4/2003

Click on the Details tab to get the more details on the certificate

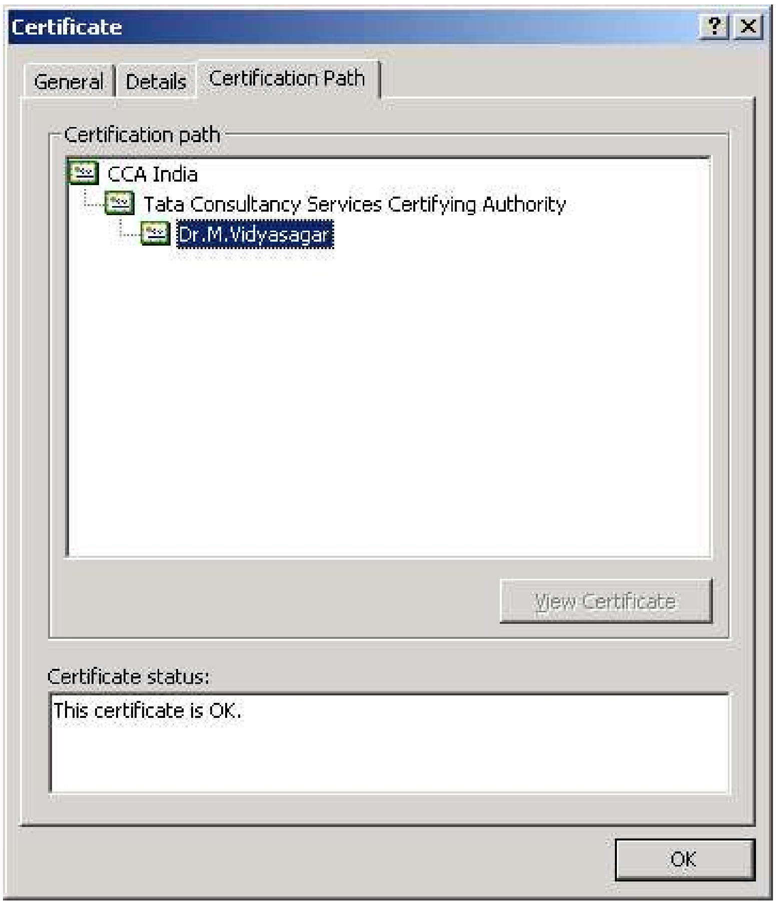


Show: <All>

Field	Value
Version	V3
Serial number	0105
Signature algorithm	sha1RSA
Issuer	AP, admin@tcs-ca.tcs.co.in, H...
Valid from	Wednesday, December 04, 20...
Valid to	Thursday, December 04, 2003...
Subject	IN, Andhra Pradesh, Hyderab...
Public key	RSA (1024 Bits)

C = IN
S = Andhra Pradesh
L = Hyderabad
OU = Class 3 Certificate
OU = Advanced Technology Centre
O = India PKI
O = Tata Consultancy Services
E = sagar@hydbad.tcs.co.in
CN = Dr.M.Vidyasagar

The Hierarchy of trust for the certificate can be seen by clicking the Certification Path tab



CCA India
Tata Consultancy Services Certifying Authority
Dr.M.Vidyasagar

Certificate status:
This certificate is OK.

In this example, the certificate is issued by TCS-CA, whose certificate is issued by CCA India.

PKCS #12 FILES

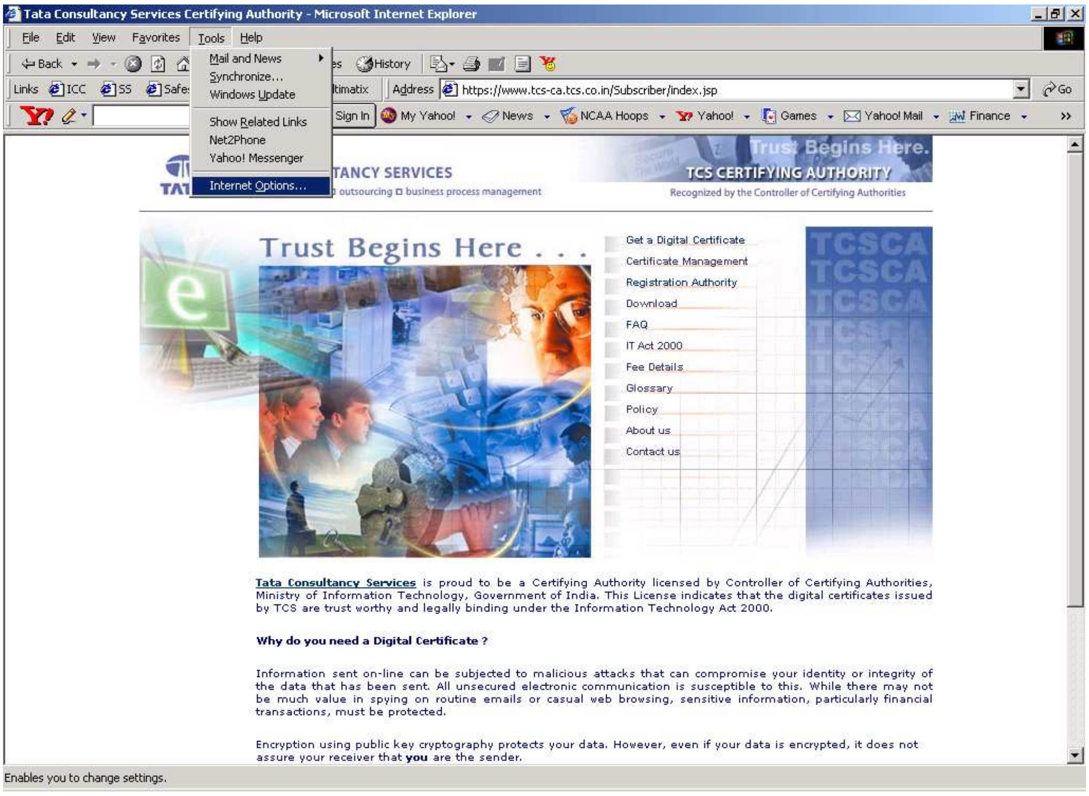
PKCS stands for Public Key Cryptographic Standard. PKCS #12 is the standard for transporting the private key along with the certificate securely. It has both the private key and the certificate. The private key is encrypted.

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



Tata Consultancy Services is proud to be a Certifying Authority licensed by Controller of Certifying Authorities, Ministry of Information Technology, Government of India. This License indicates that the digital certificates issued by TCS are trust worthy and legally binding under the Information Technology Act 2000.

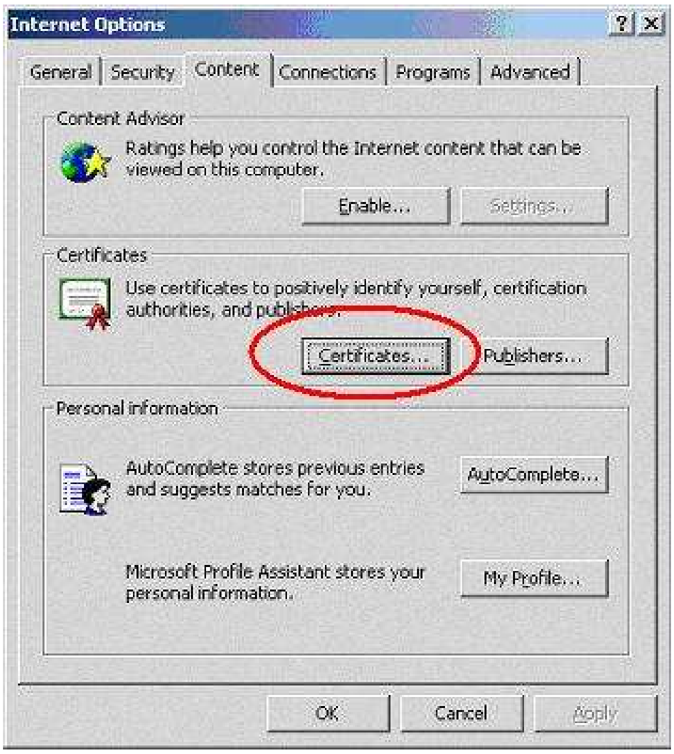
Why do you need a Digital Certificate ?

Information sent on-line can be subjected to malicious attacks that can compromise your identity or integrity of the data that has been sent. All unsecured electronic communication is susceptible to this. While there may not be much value in spying on routine emails or casual web browsing, sensitive information, particularly financial transactions, must be protected.

Encryption using public key cryptography protects your data. However, even if your data is encrypted, it does not assure your receiver that **you** are the sender.

Enables you to change settings.

2. Click on the “Content -> Certificates” tab on the dialogue box shown.



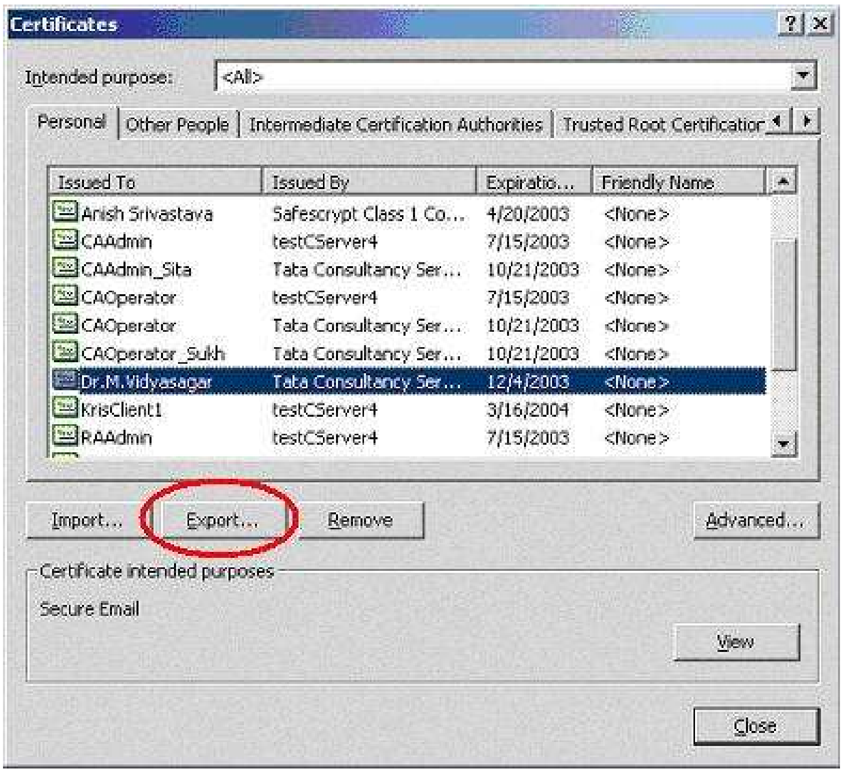
Ratings help you control the Internet content that can be viewed on this computer.

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.

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

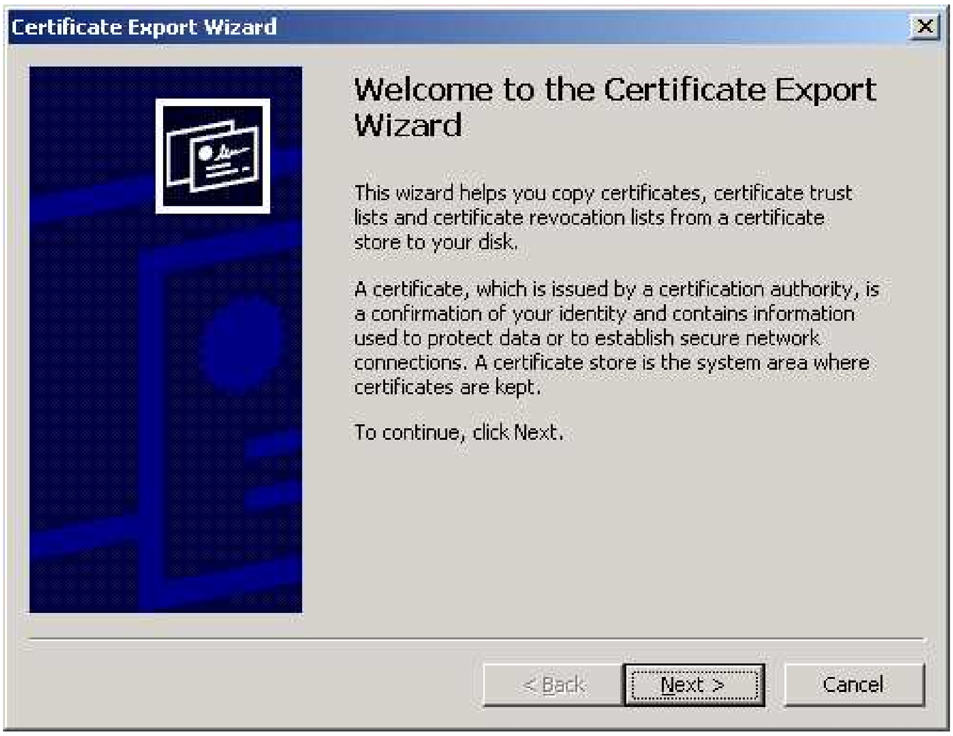

Certificates
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Anish Srivastava	Safescrypt Class 1 Co...	4/20/2003	<None>
CAAdmin	testCServer4	7/15/2003	<None>
CAAdmin_Sita	Tata Consultancy Ser...	10/21/2003	<None>
CAOperator	testCServer4	7/15/2003	<None>
CAOperator	Tata Consultancy Ser...	10/21/2003	<None>
CAOperator_Sukh	Tata Consultancy Ser...	10/21/2003	<None>
Dr.M.Vidyasagar	Tata Consultancy Ser...	12/4/2003	<None>
KrisClient1	testCServer4	3/16/2004	<None>
RAAdmin	testCServer4	7/15/2003	<None>

Secure Email

4. Click Next to the dialogue to continue



Certificate Export Wizard

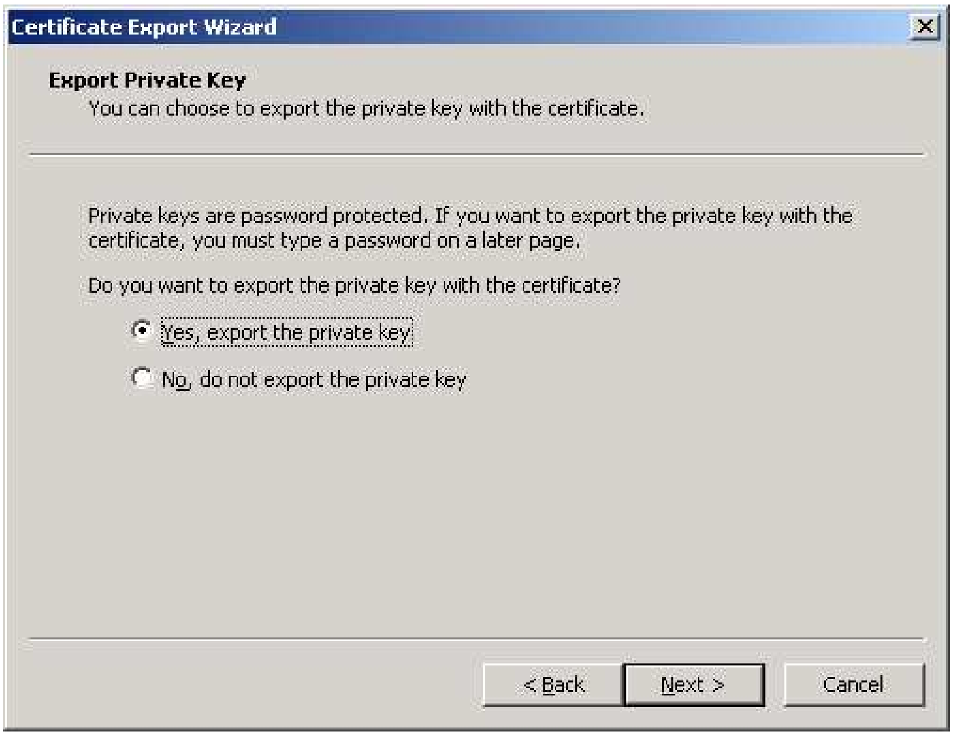
Welcome to the Certificate Export Wizard

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.

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



Certificate Export Wizard

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

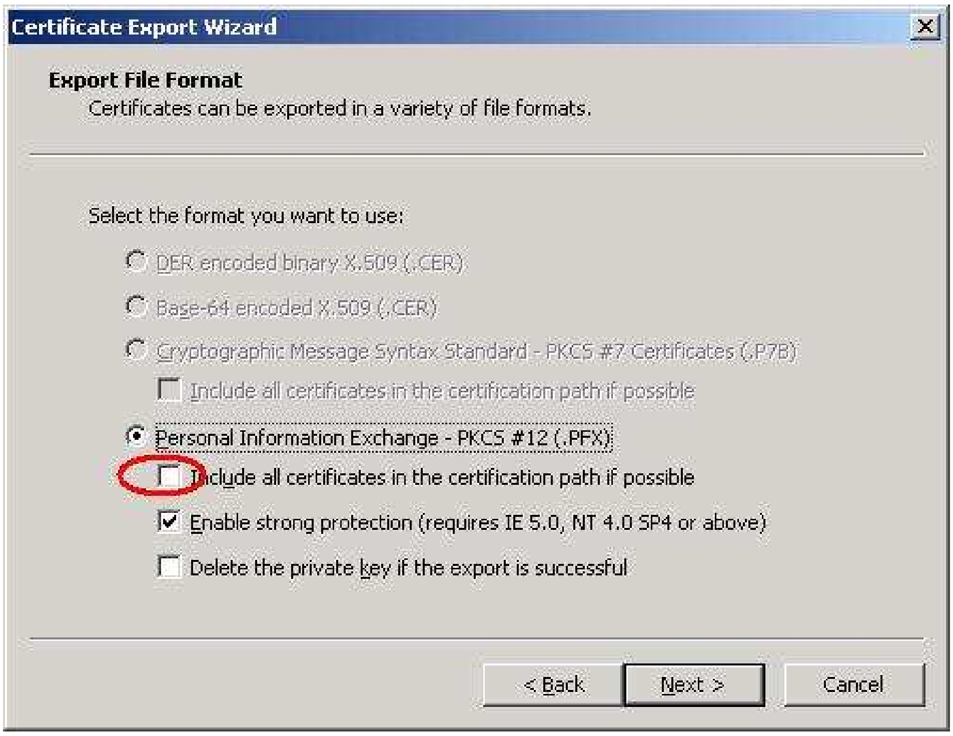
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

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

● Yes, export the private key

○ No, do not export the private key

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

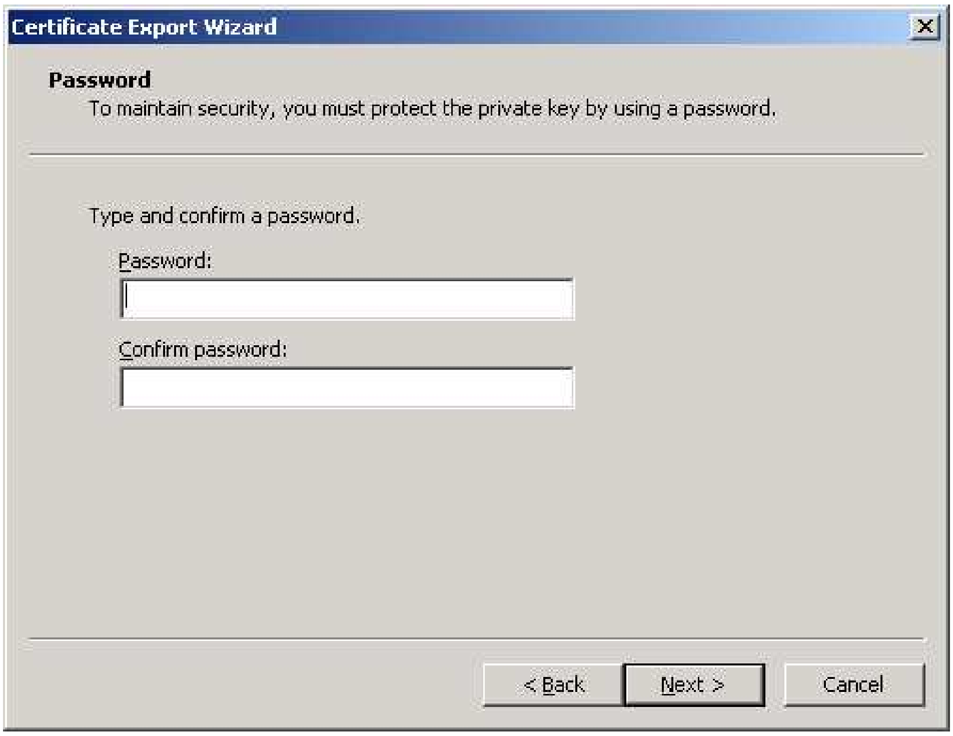
● Personal Information Exchange - PKCS #12 (.PFX)

□ 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

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



Certificate Export Wizard

Password

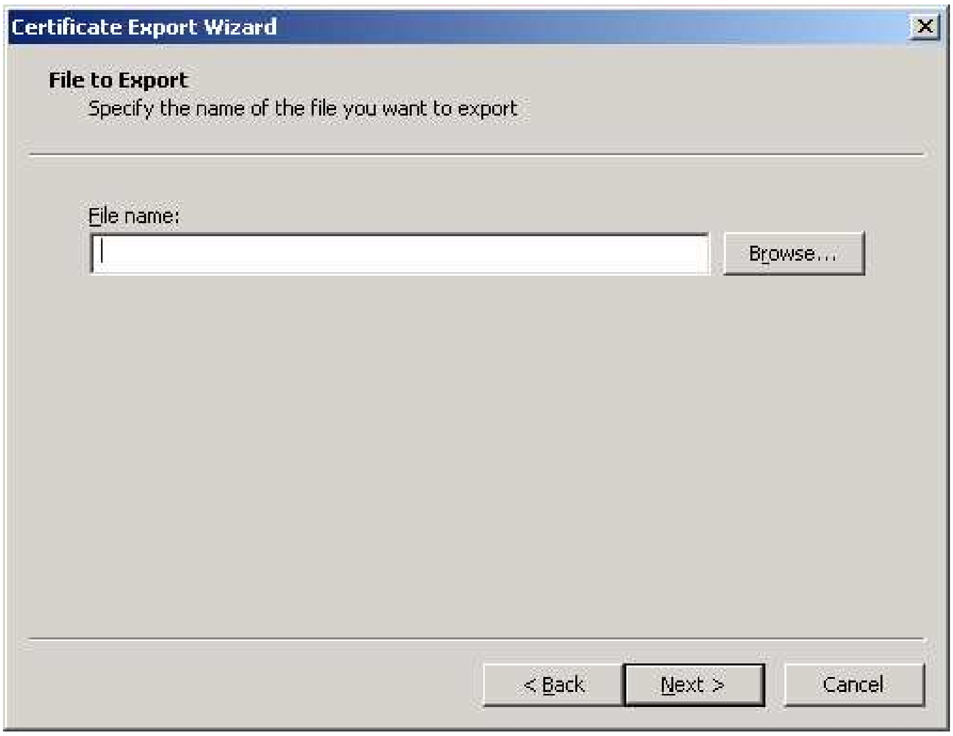
To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password:

Confirm password:

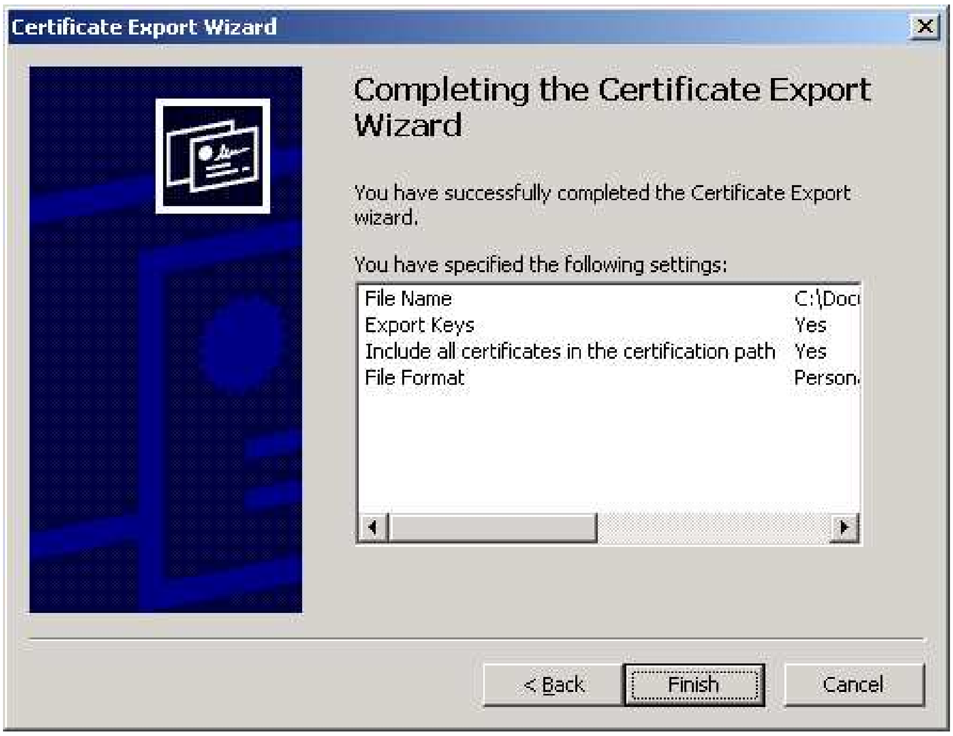
8. Choose the file name and location to save the file. Give the extension of the file as ".p12" or ".pfx"



File to Export
Specify the name of the file you want to export

File name:

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



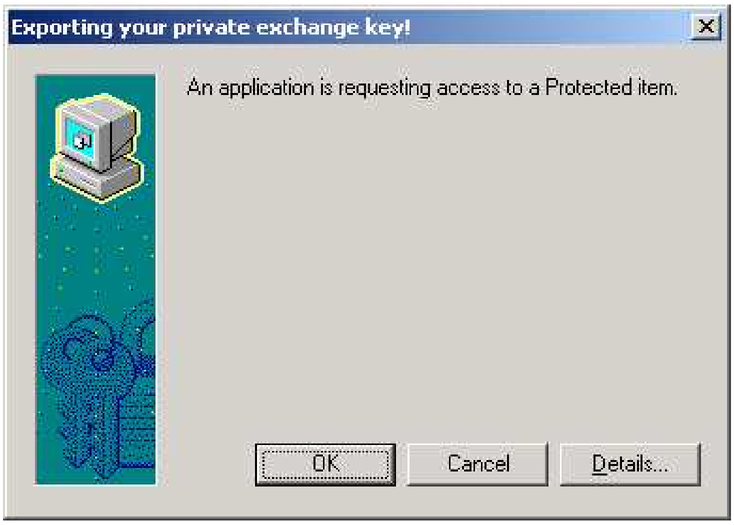
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

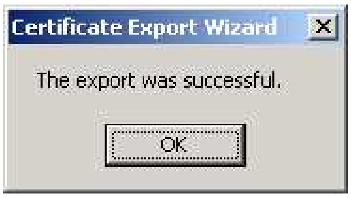
File Name	C:\Doc
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Person

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



An application is requesting access to a Protected item.

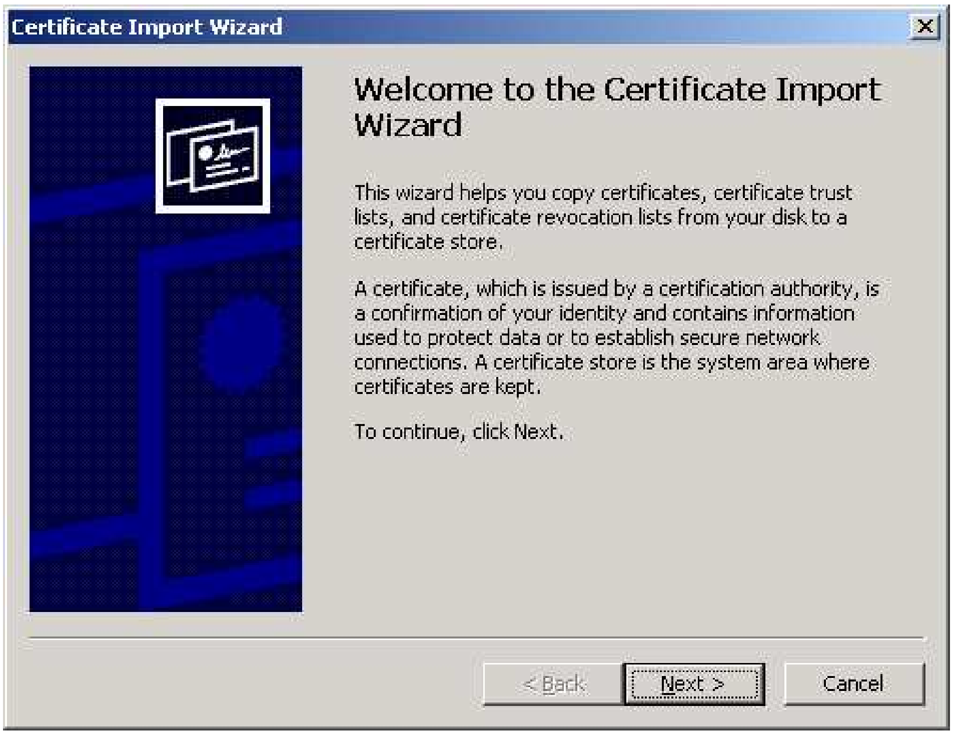
11. A message will be shown indicating the successful completion of the export



The export was successful.

IMPORTING THE PKCS #12 FILE INTO THE BROWSER

1. Double-click on the “.p12” or “.pfx” file.
2. Click “Next” on the dialogue to continue



Certificate Import Wizard

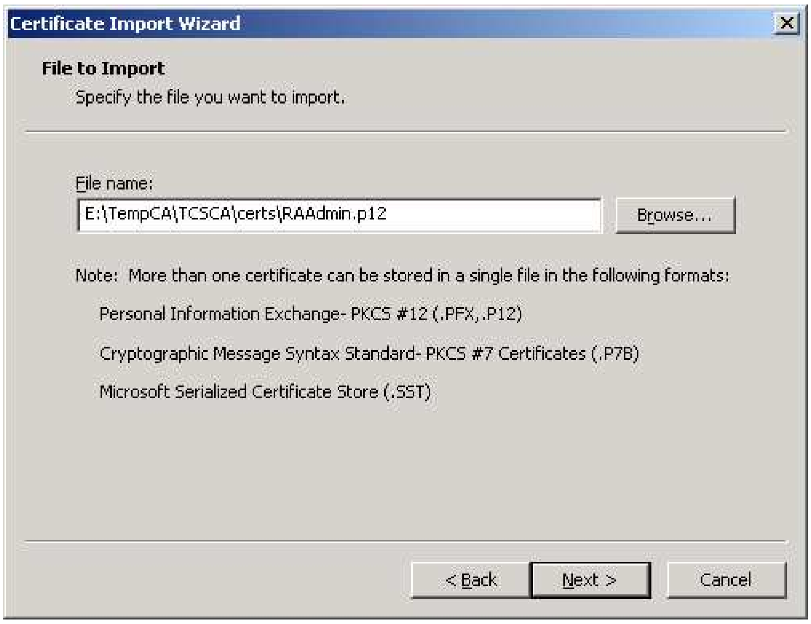
Welcome to the Certificate Import Wizard

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

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.

3. Check the File location and click “Next”



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

E:\TempCA\TCSCA\certs\RAAdmin.p12

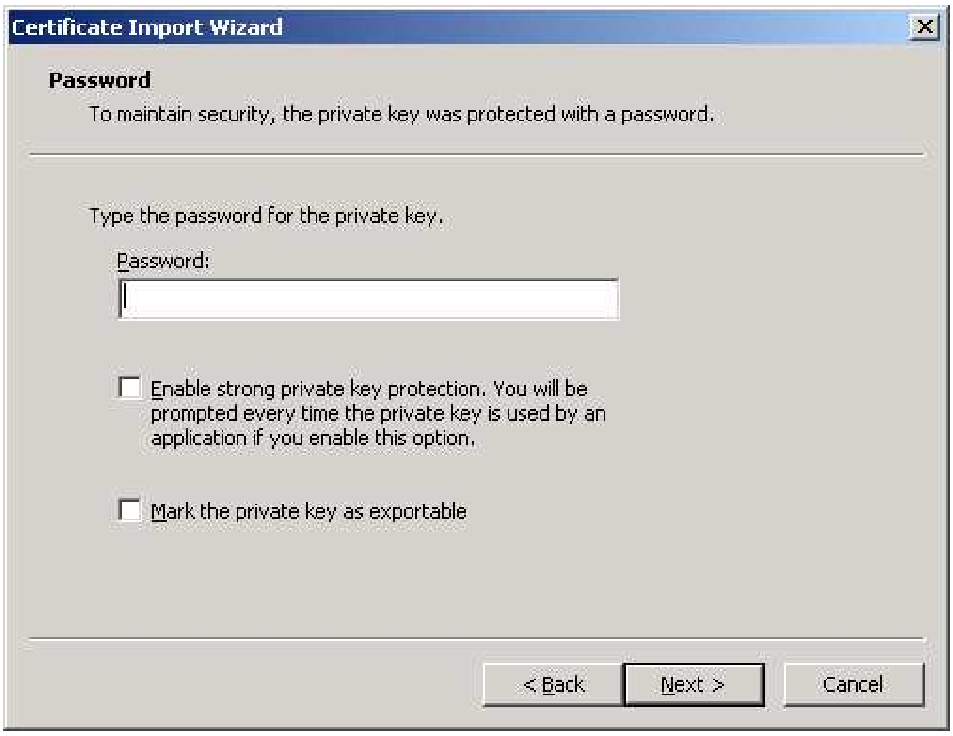
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

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

Microsoft Serialized Certificate Store (.SST)

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



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

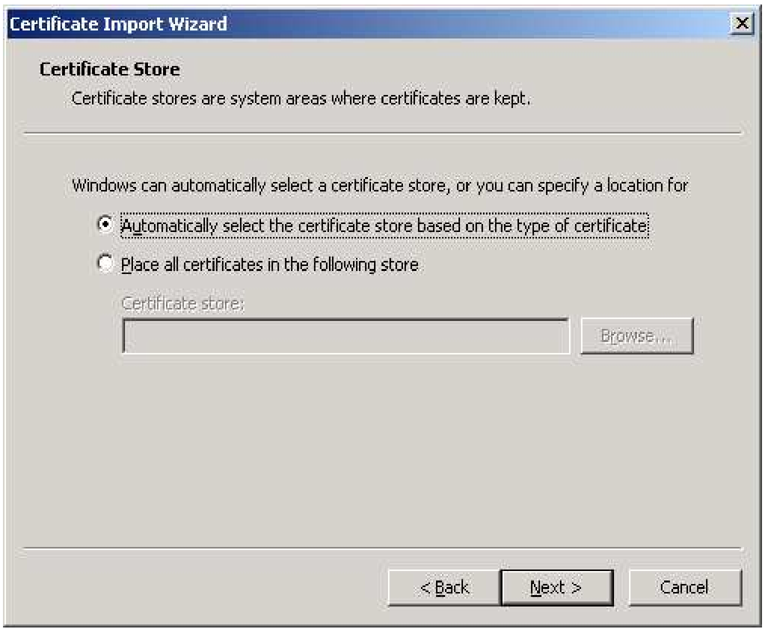
Password:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark the private key as exportable

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.

5. Choose the option to automatically select the certificate store as shown and click ‘Next”



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

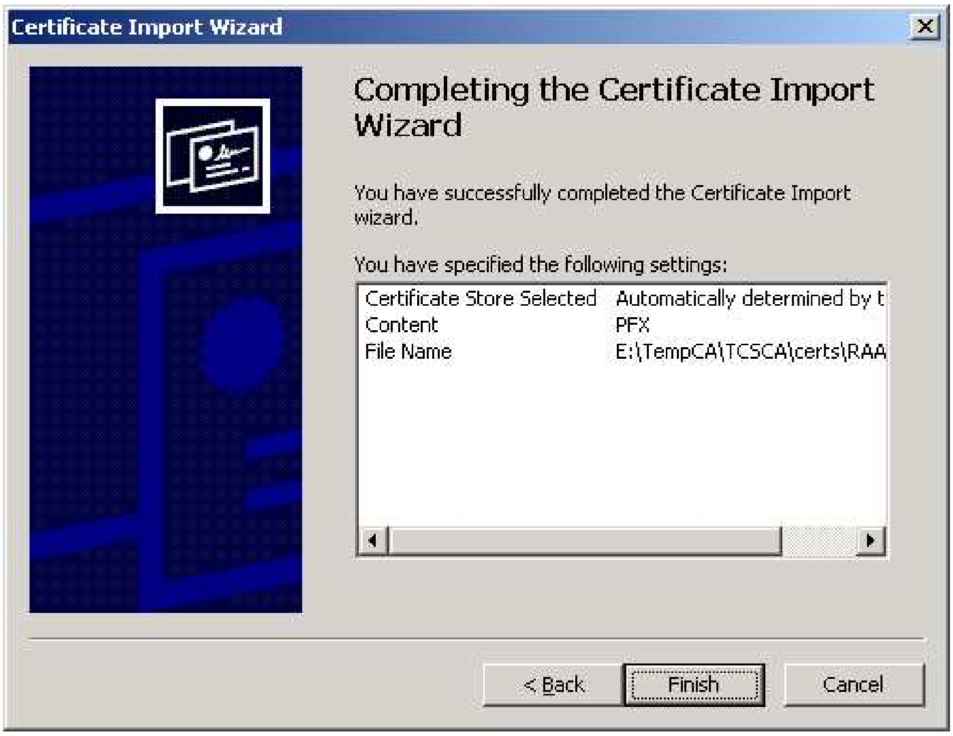
Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

6. Click “Finish” to import the PKCS #12 file



Certificate Import Wizard

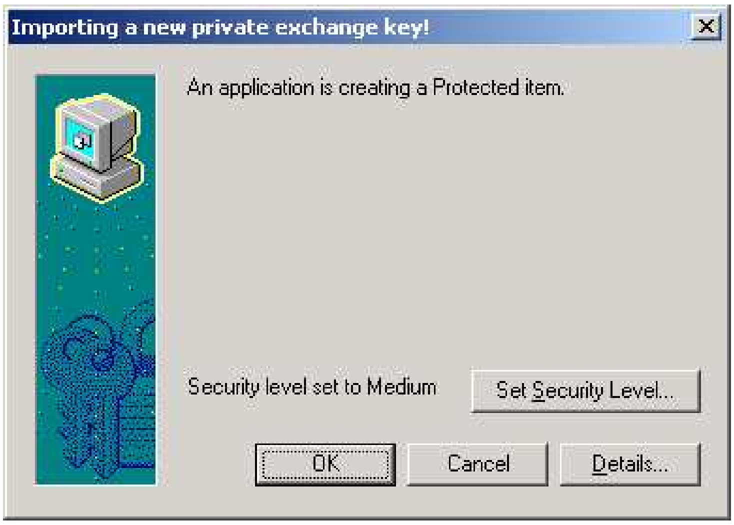
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	E:\TempCA\TCSCA\certs\RAA

7. Click “OK” to import the private key

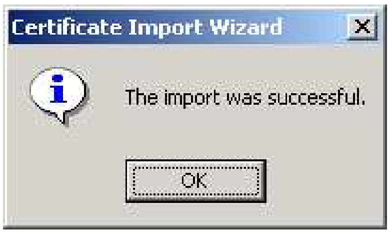


Importing a new private exchange key!

An application is creating a Protected item.

Security level set to Medium

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



Certificate Import Wizard

The import was successful.

*****End of Document*****