DohatecCA
Certifying Authority

Dohatec CA

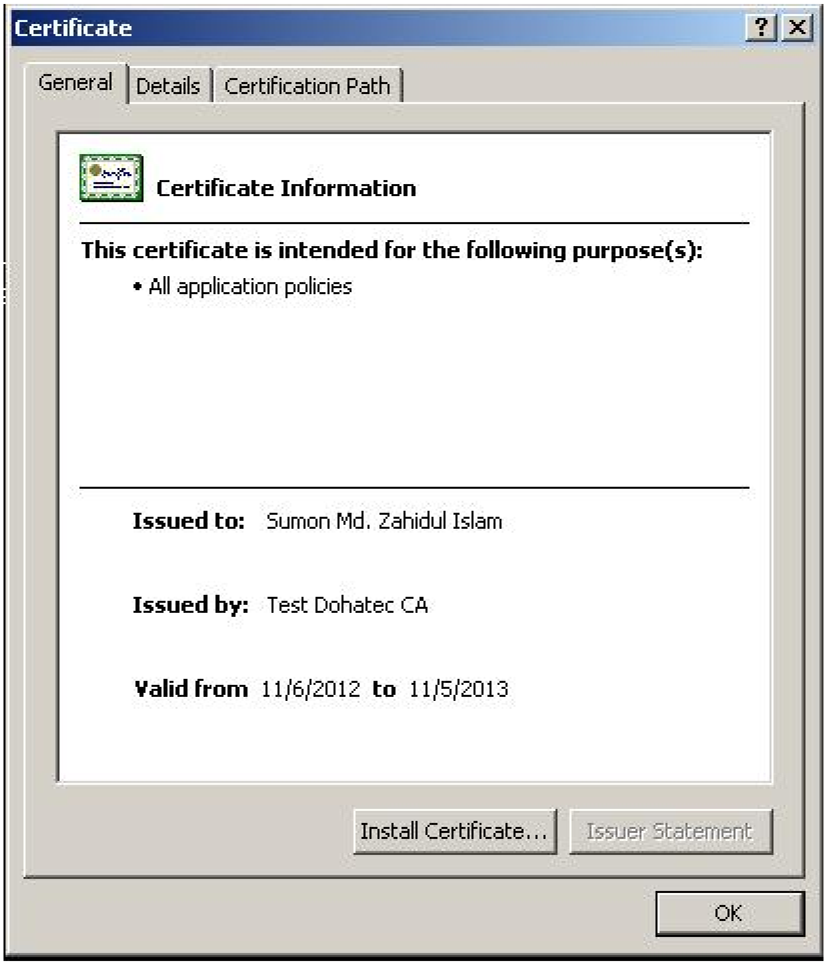
Export/Import Procedure eToken Pro 72K

FOR USERS OF ETOKENS

[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.



Certificate Information

This certificate is intended for the following purpose(s):

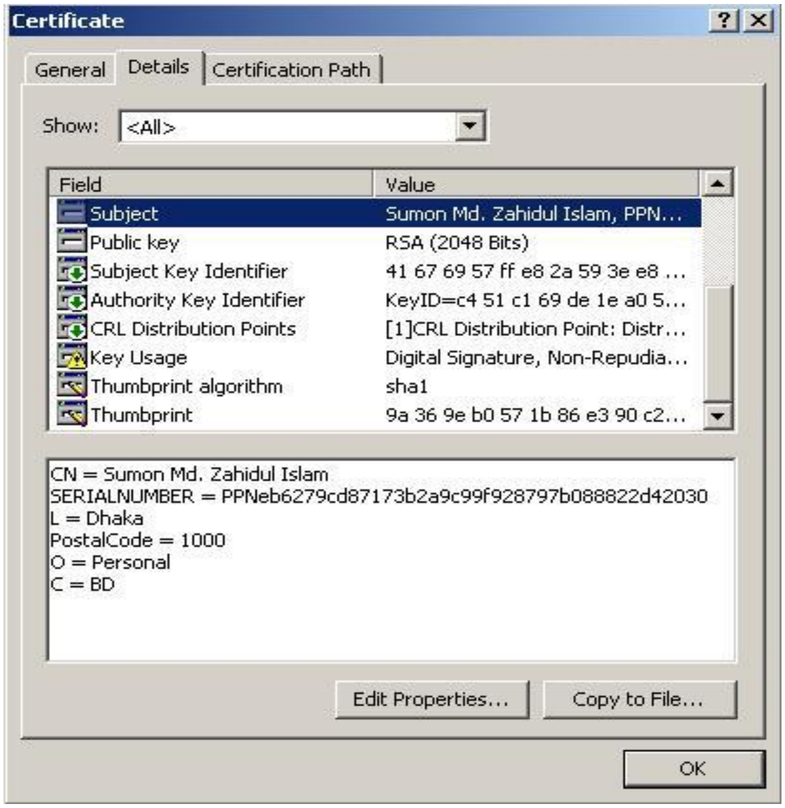
- All application policies

Issued to: Sumon Md. Zahidul Islam

Issued by: Test Dohatec CA

Valid from 11/6/2012 **to** 11/5/2013

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

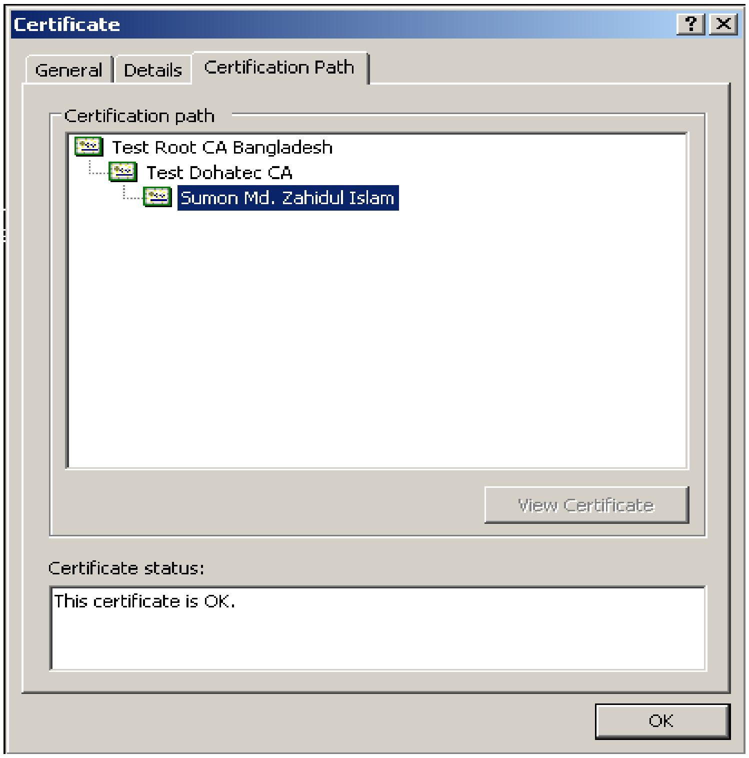


Show: <All>

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

- ➢ The hierarchy of trust for a certificate can be seen by clicking the ‘Certification Path’ tab.



Certification path

Test Root CA Bangladesh
Test Dohatec CA
Sumon Md. Zahidul Islam

Certificate status:

This certificate is OK.

In this example, the certificate is issued by Dohatec CA, whose certificate is issued by CCA Bangladesh.

2 PKCS #12 Files

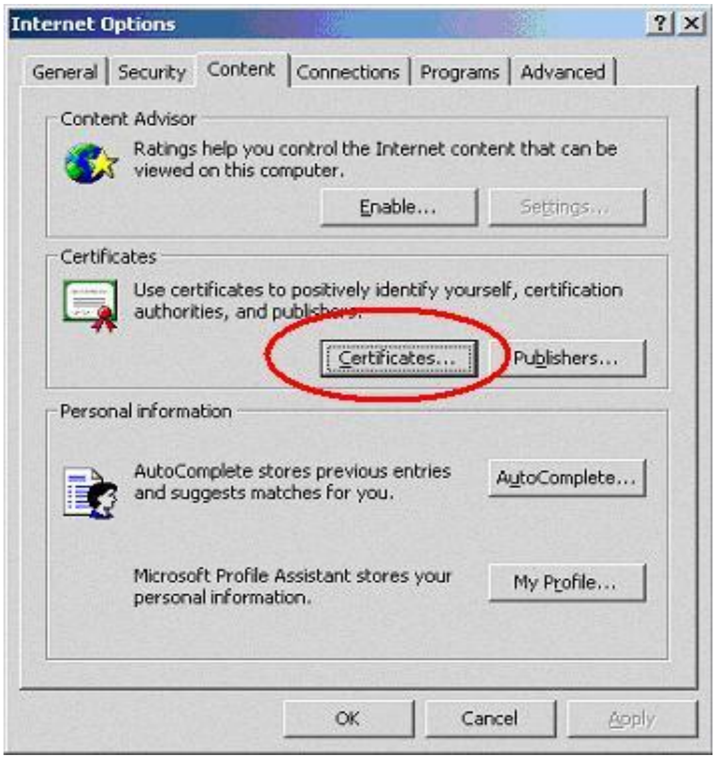
PKCS stands for Public Key Cryptographic Standard. PKCS #12 is the standard for transporting the private key along with the certificate securely. It has both the private key and the certificate. The private key is encrypted.

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



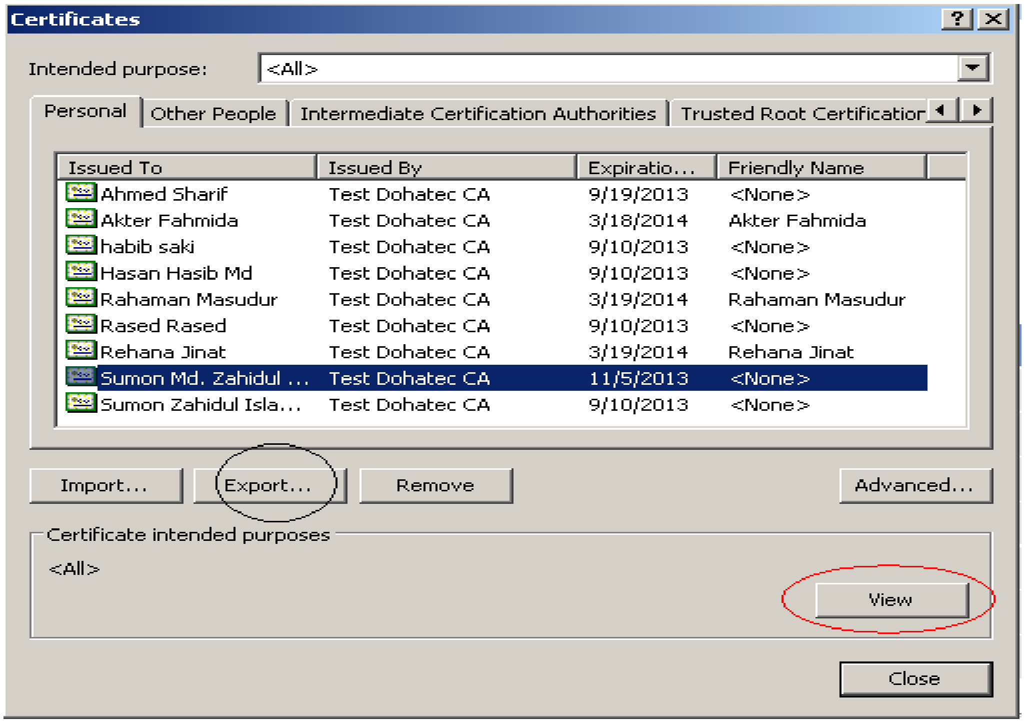
Ratings help you control the Internet content that can be viewed on this computer.

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.

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



Certificates

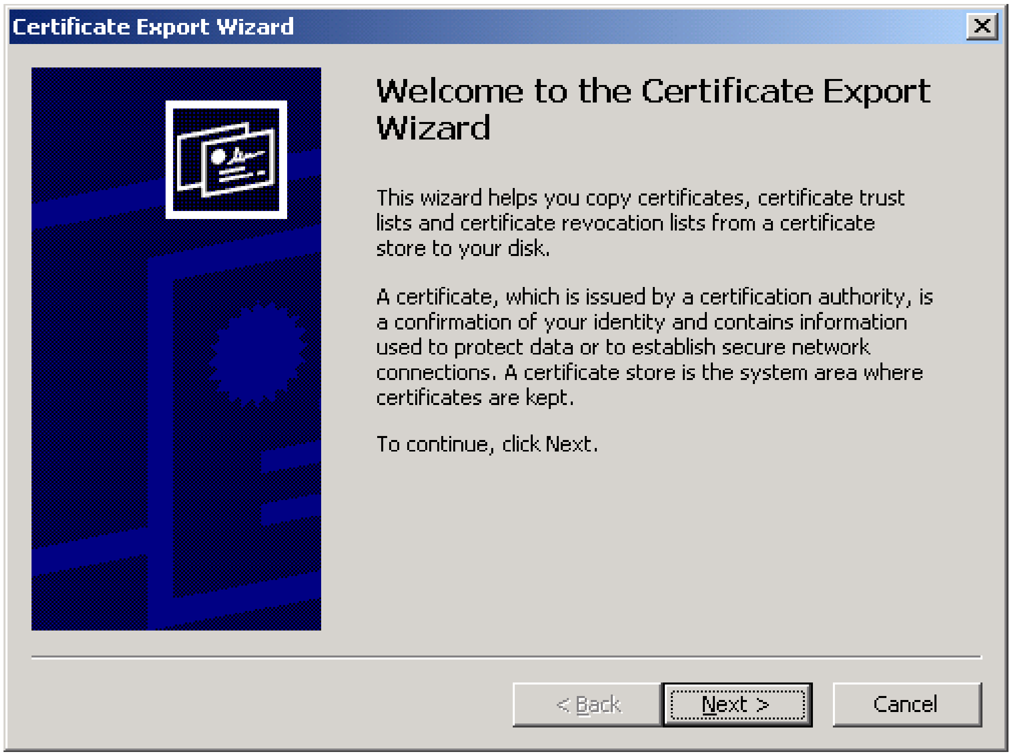
Intended purpose: <All>

Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification

Issued To	Issued By	Expiratio...	Friendly Name
Ahmed Sharif	Test Dohatec CA	9/19/2013	<None>
Akter Fahmida	Test Dohatec CA	3/18/2014	Akter Fahmida
habib saki	Test Dohatec CA	9/10/2013	<None>
Hasan Hasib Md	Test Dohatec CA	9/10/2013	<None>
Rahaman Masudur	Test Dohatec CA	3/19/2014	Rahaman Masudur
Rased Rased	Test Dohatec CA	9/10/2013	<None>
Rehana Jinat	Test Dohatec CA	3/19/2014	Rehana Jinat
Sumon Md. Zahidul ...	Test Dohatec CA	11/5/2013	<None>
Sumon Zahidul Isla...	Test Dohatec CA	9/10/2013	<None>

Certificate intended purposes
<All>

- Click Next to the dialog to continue.



Certificate Export Wizard

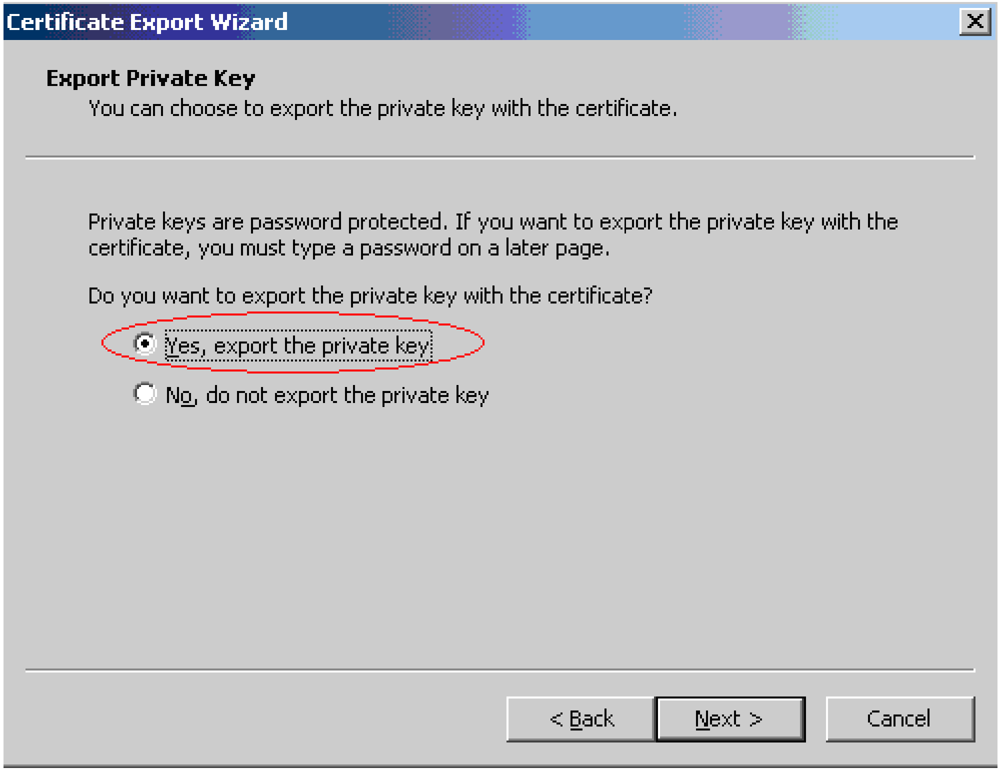
Welcome to the Certificate Export Wizard

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.

- 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.

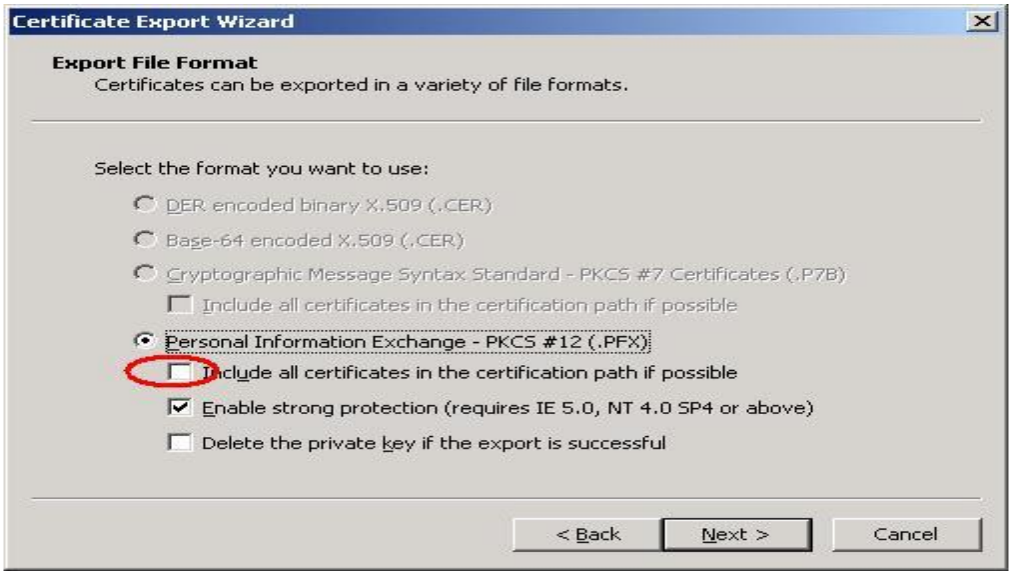
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

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

● Yes, export the private key

○ No, do not export the private key

- 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

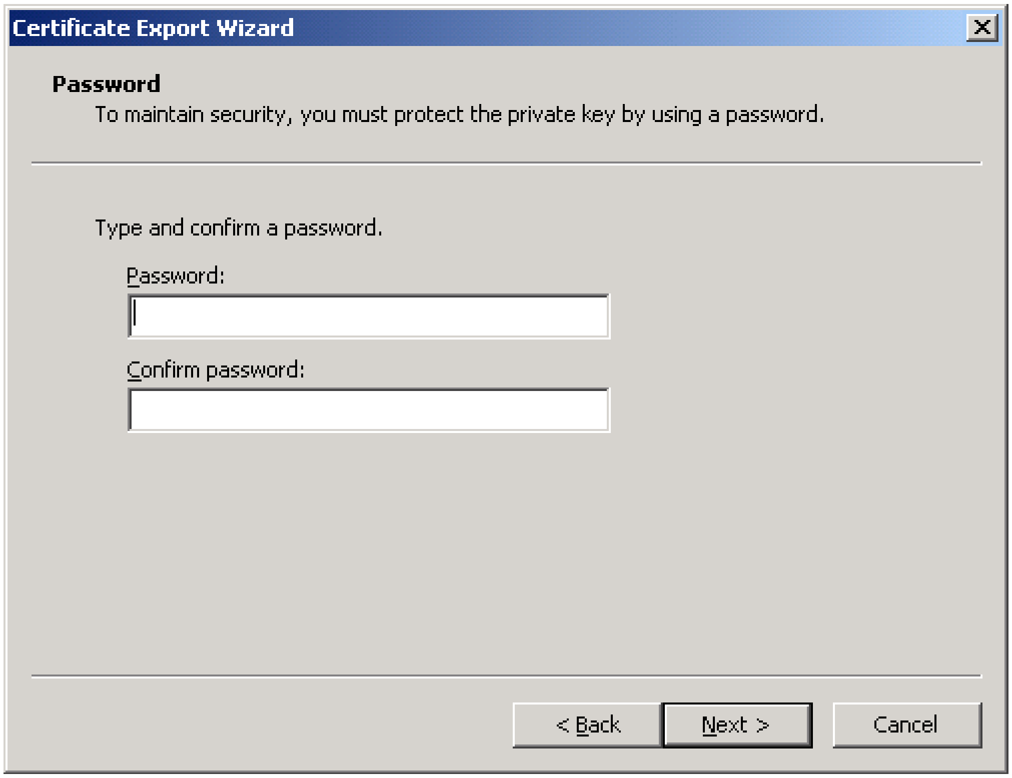
● Personal Information Exchange - PKCS #12 (.PFX)

□ 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

- Enter the password to protect the PKCS#12 file



Certificate Export Wizard

Password

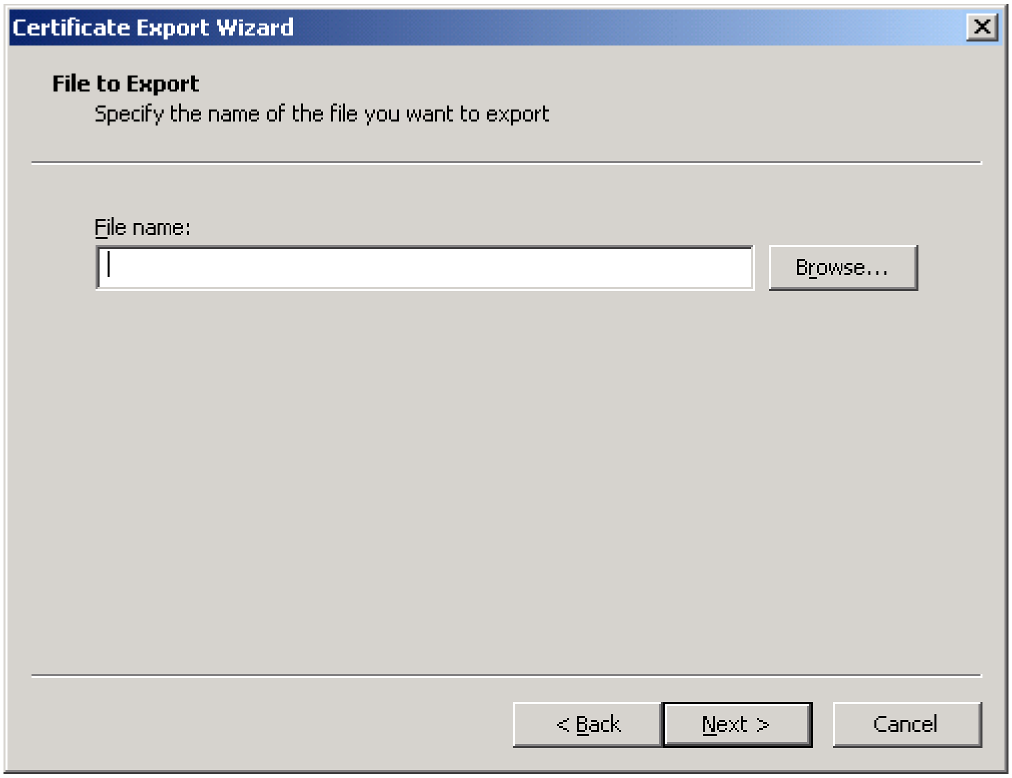
To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password:

Confirm password:

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



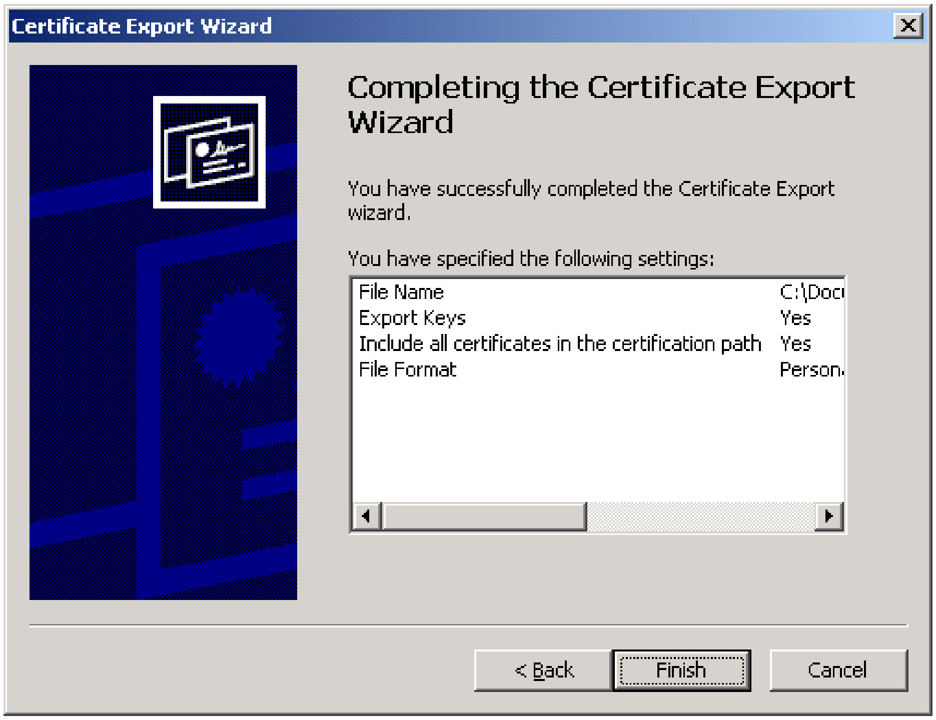
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

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



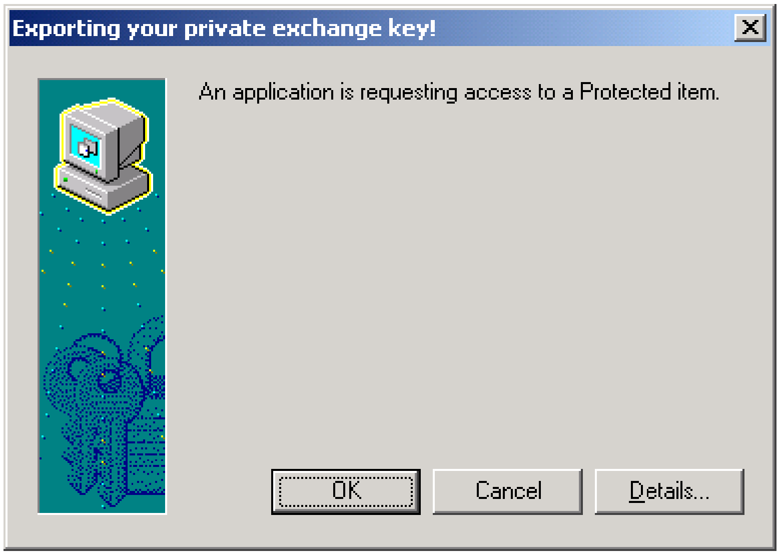
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

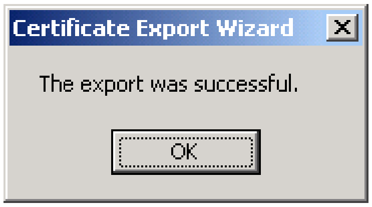
File Name	C:\Doc
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Person

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



An application is requesting access to a Protected item.

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



The export was successful.

2.2 Importing PKCS#12 Form into the eToken

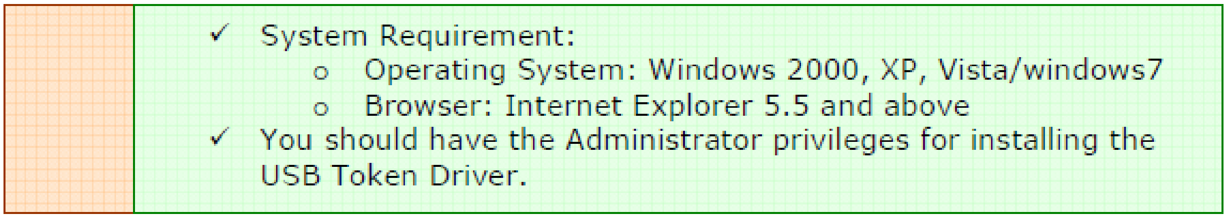
Getting Started

To start the process, procure the Digital Certificate Enrollment Kit from Dohatec CA or its Registration Authorities. The kit contains:

- USB Token (Safenet eToken pro 72K)
- Installation CD contains:
  - USB Drivers

Note:

- *Use the Installation CD to install the USB Token driver.*
- *Ensure the following before installing the USB token driver.*

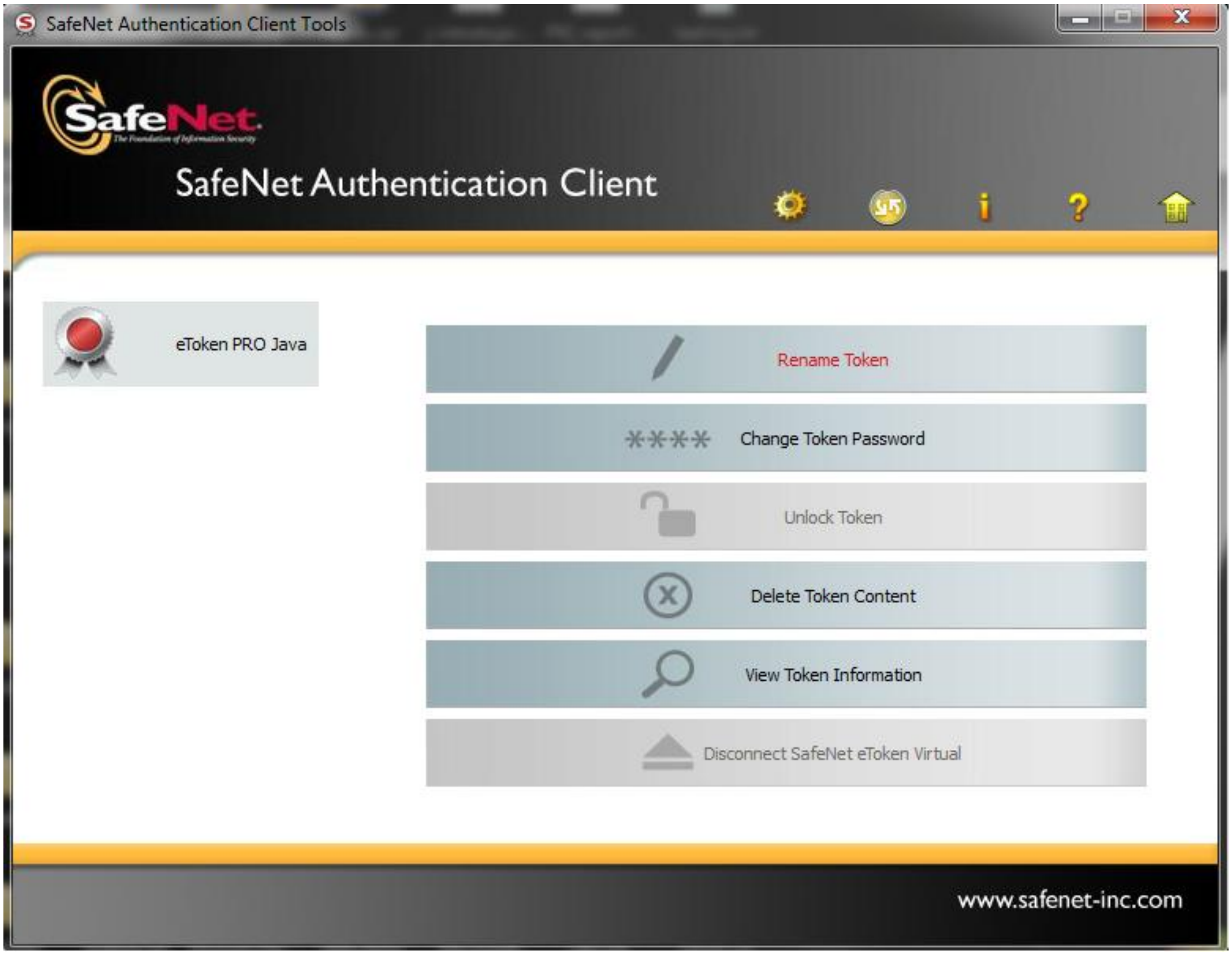


✓ System Requirement:
  - Operating System: Windows 2000, XP, Vista/windows7
  - Browser: Internet Explorer 5.5 and above

✓ You should have the Administrator privileges for installing the USB Token Driver.

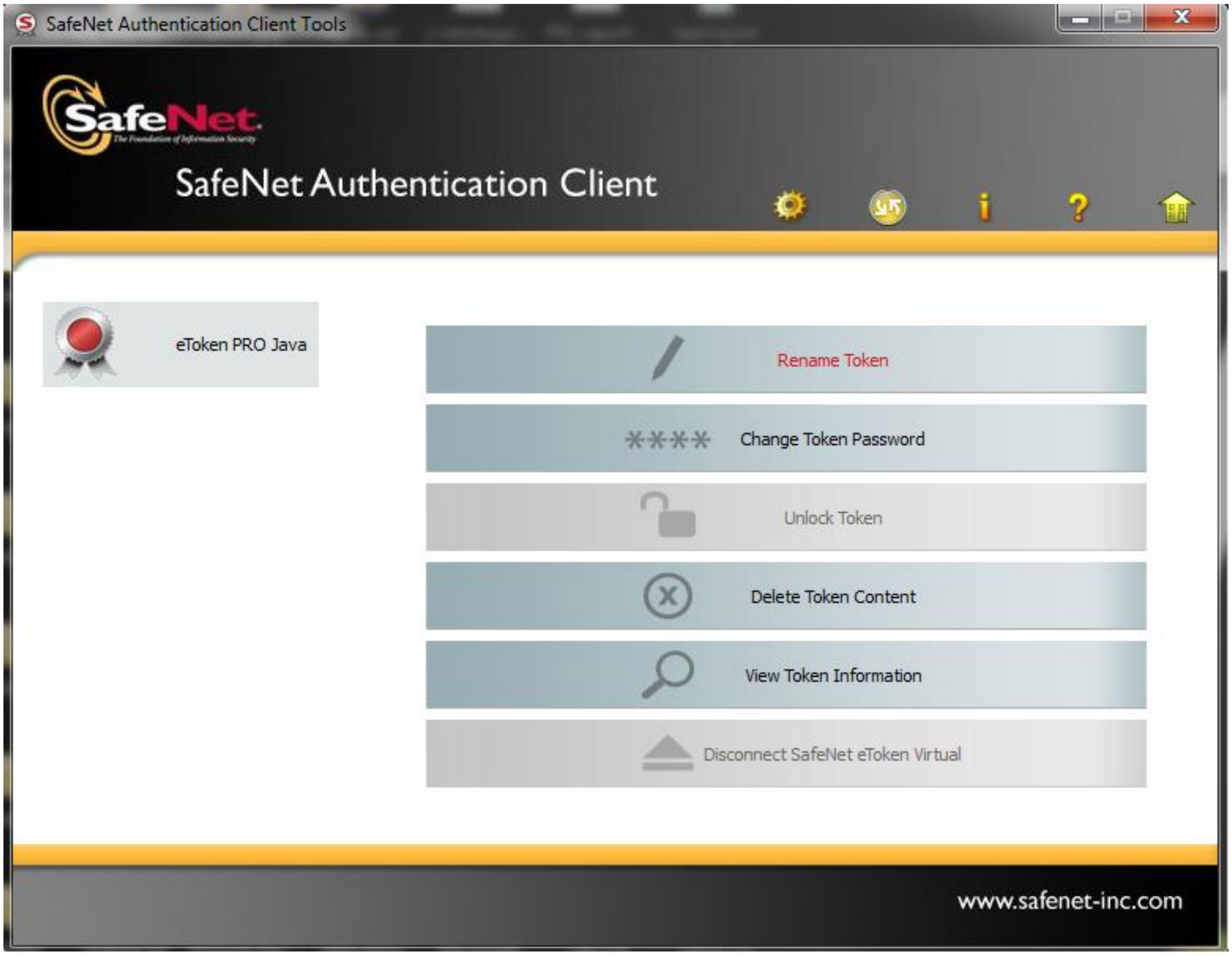
1. To install eToken Pro 72K drivers, insert the CD.
2. Click on the Windows Installer Package named **‘SafeNetAuthenticationClient-x32-x64-8.1-SP1.exe’**, (if the OS is 32/64 bit then click on ‘**SafeNetAuthenticationClient-x32-x64-8.1-SP1.exe’**) accept the License Agreement and proceed with installation.
3. Insert the eToken USB Token in the USB port of the computer, if prompted
4. Restart the computer after the installation is complete.

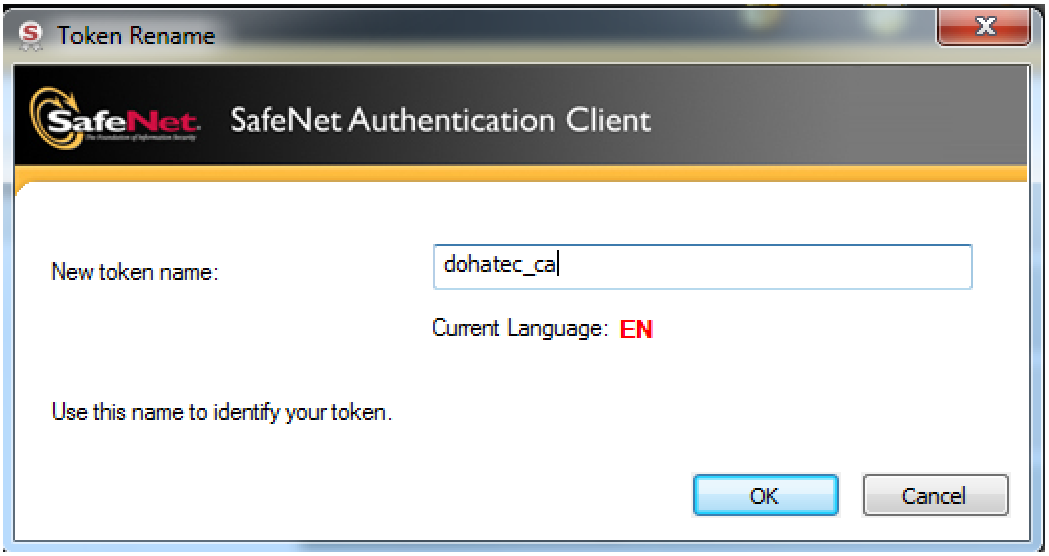
After completing the installation process now go to **Start** > **All Programs** > **Safenet** > **Safenet Authentication Client** > **Safenet Authentication Client Tools** with your eToken inserted, the following screen is displayed.


SafeNet Authentication Client Tools
SafeNet
The Foundation of Information Security
SafeNet Authentication Client
eToken PRO Java
Rename Token
Change Token Password
Unlock Token
Delete Token Content
View Token Information
Disconnect SafeNet eToken Virtual
www.safenet-inc.com

Renaming the eToken:

For additional convenience and ease of identification, the eToken names can also be personalized. Click “Rename eToken” on the eToken Properties screen.





New token name: dohatec_ca

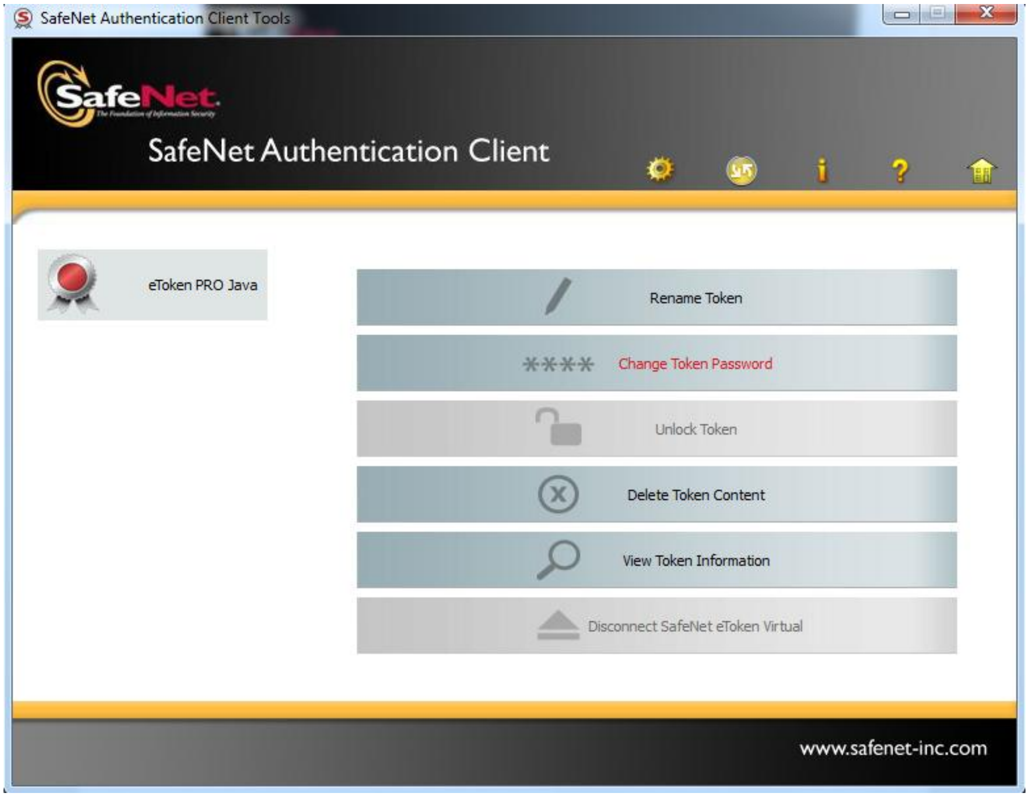
Current Language: EN

Use this name to identify your token.

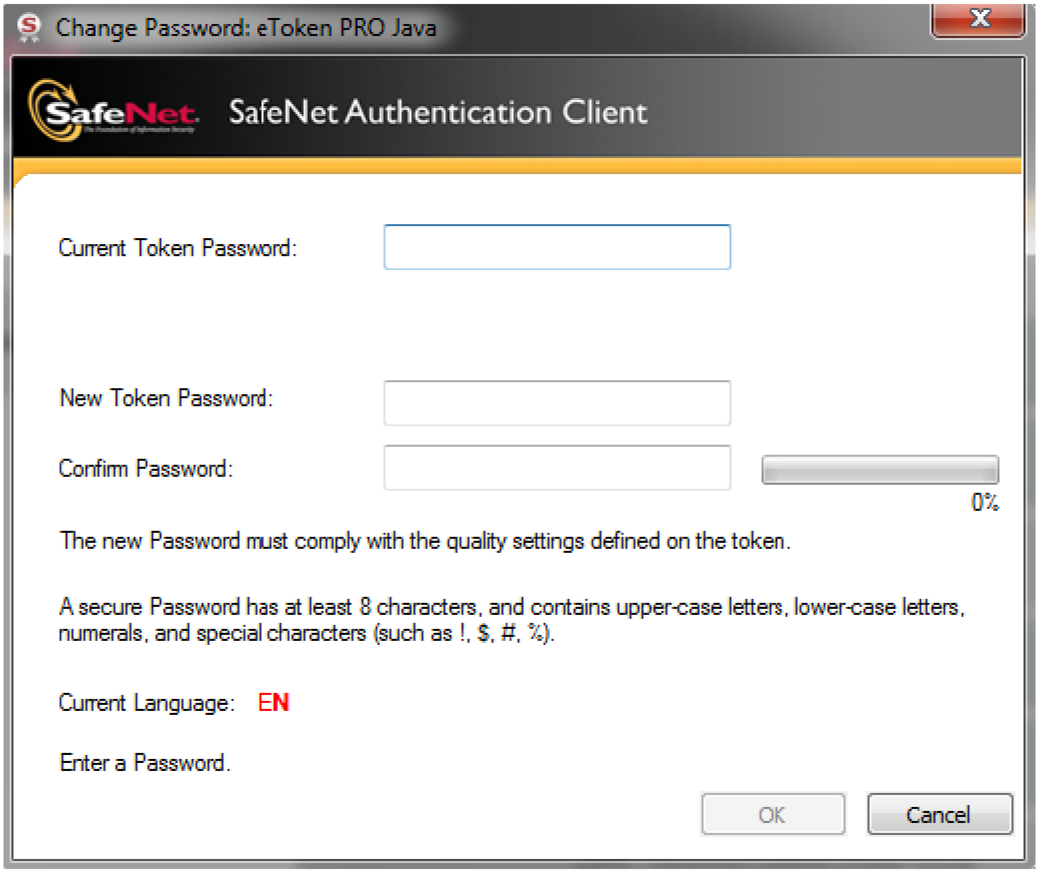
- Enter the new eToken name in the eToken name field and click on "OK" to set the eToken name.
- Click “OK” and in the eToken Properties window the new eToken name is displayed

Changing the eToken Password:

All eTokens are configured at manufacture with the factory default password. This password is normally “1234567890”. Click “Change eToken password” on the eToken Properties screen and the following eToken Properties dialog is displayed:



Enter your current eToken password in the “Current Token Password” field and, the new password in the “New Token Password” field. Confirm new Password and click “OK” to set the new Password.



Change Password: eToken PRO Java

SafeNet Authentication Client

Current Token Password:

New Token Password:

Confirm Password:

The new Password must comply with the quality settings defined on the token.

A secure Password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, $, #, %).

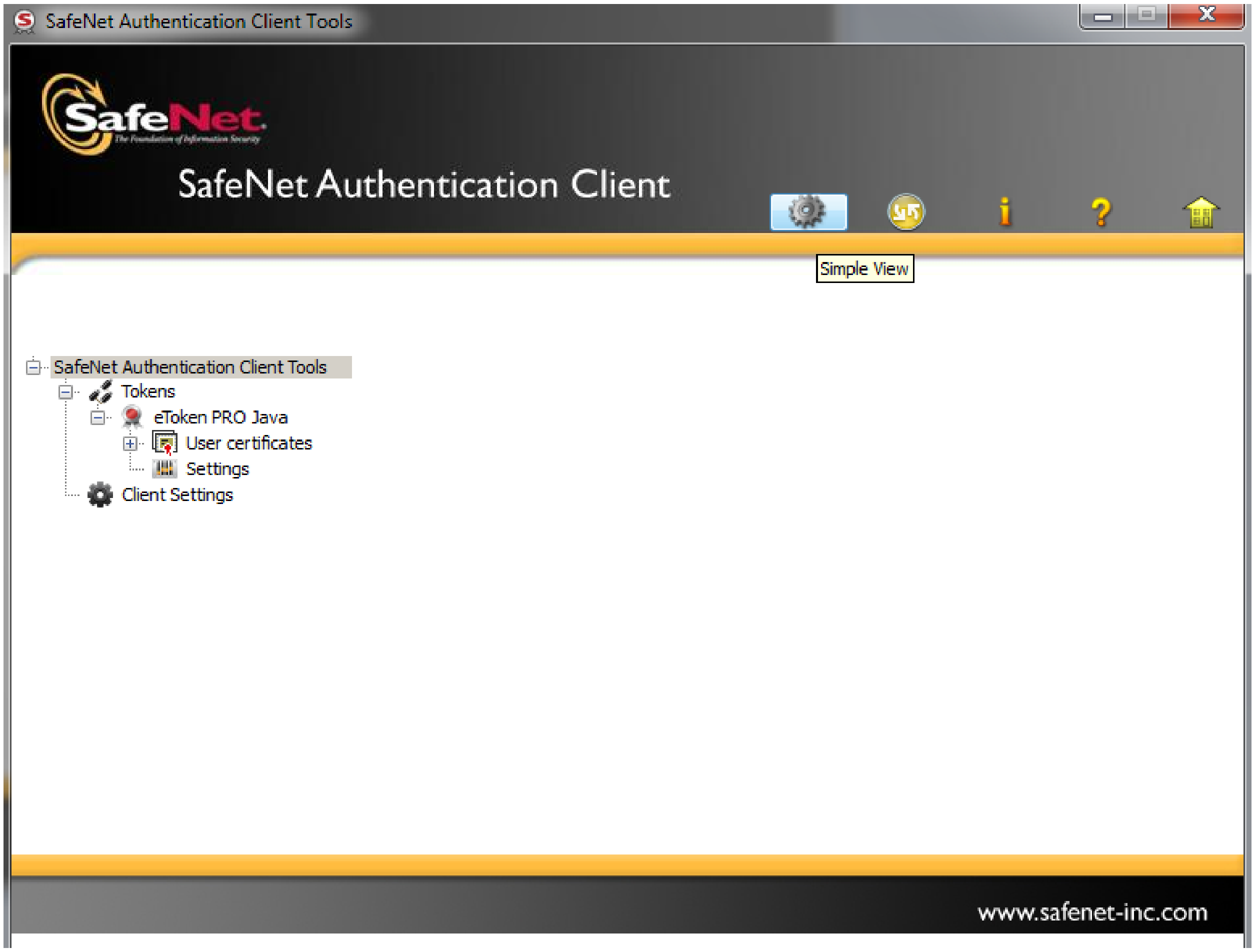
Current Language: EN

Enter a Password.

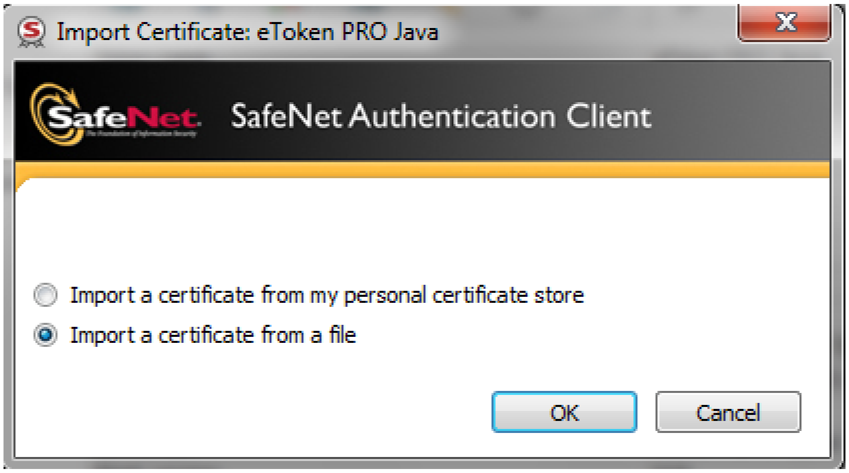
Import Procedure:

Select the ‘Advanced’ option on the Token properties screen. If password is necessary then provide the Token password to login and start importing the certificate.

- Right click on eToken name (here eToken Pro Java) then click "Import certificate" to import your certificate from ".PFX file" from a location on your Computer.


SafeNet Authentication Client Tools
SafeNet
SafeNet Authentication Client
Simple View
SafeNet Authentication Client Tools
Tokens
eToken PRO Java
User certificates
Settings
Client Settings
www.safenet-inc.com

- Select “Import certificate from the file” and click “OK”.



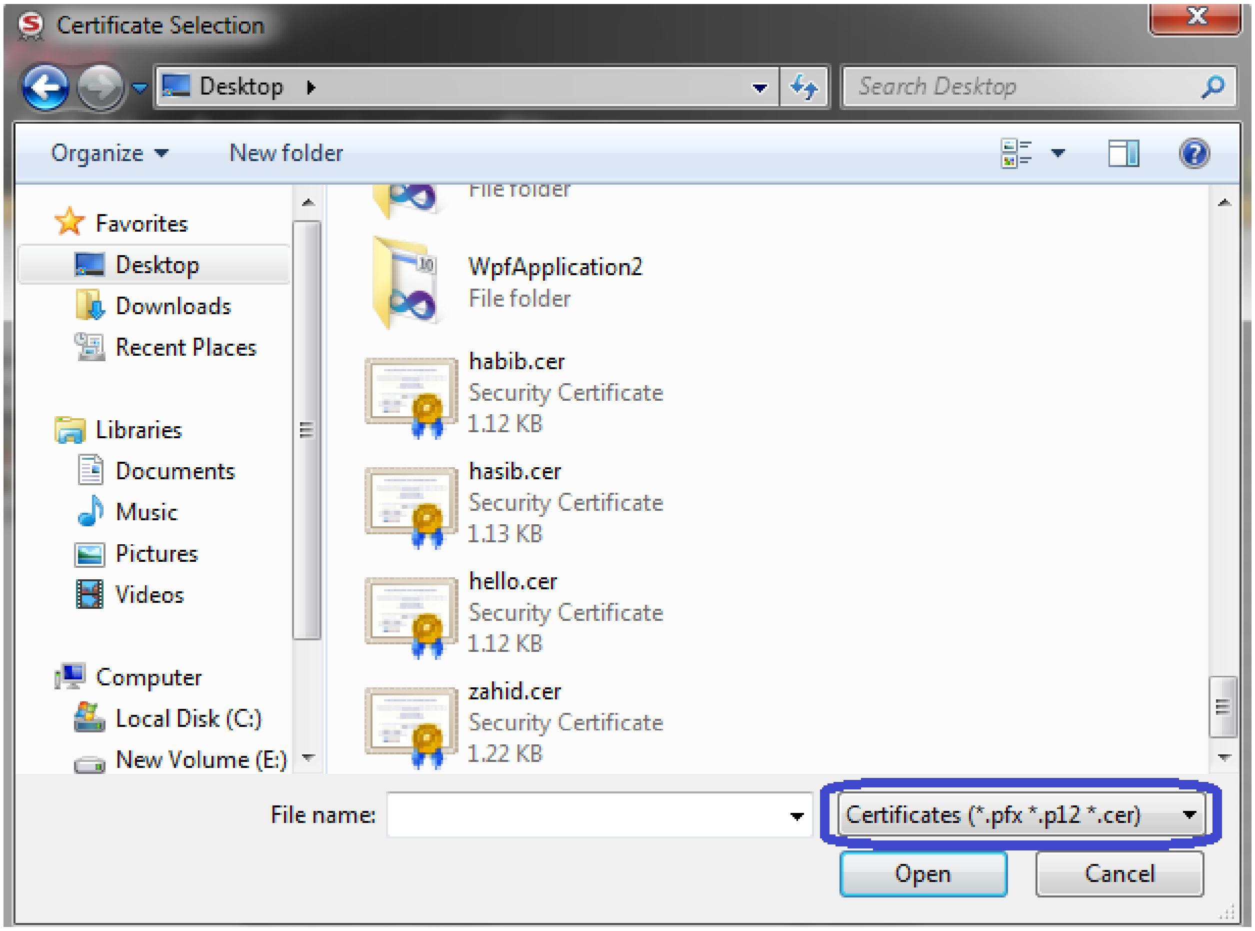
Import Certificate: eToken PRO Java

SafeNet Authentication Client

○ Import a certificate from my personal certificate store

● Import a certificate from a file

- Select the path of the ".Pfx" file and click "OK".

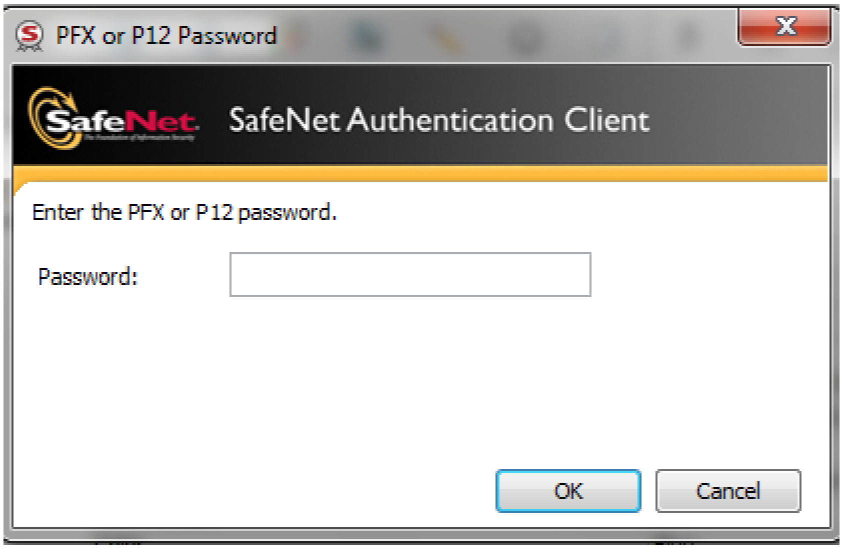


Certificate Selection

File name:

Certificates (*.pfx *.p12 *.cer)

- A prompt for Password for the private key appears. Give the password that you had set to protect the file, while exporting the certificate and click "OK"



PFX or P12 Password

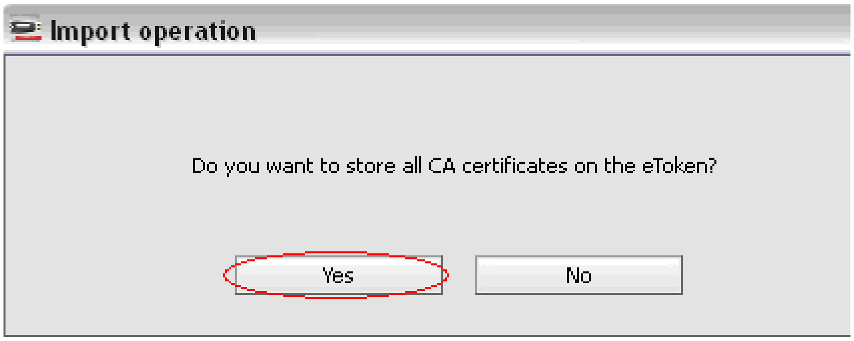
SafeNet Authentication Client

Enter the PFX or P12 password.

Password:

A certificate that is stored on the computer may be part of a hierarchical structure with more than one Certificate in the chain up to the Root CA. Importing a CA Chain takes the CA certificate and the complete CA Chain up to the root certificate that is stored on the computer and places it on the eToken.

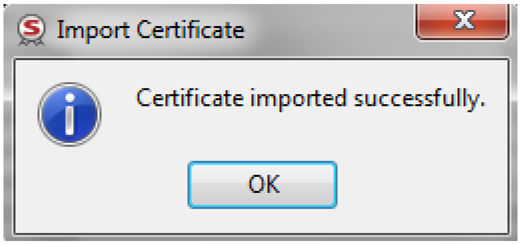
- When the certificate is imported onto the eToken the following message confirming the import the CA certificates. Click on 'Yes' to import the Root certificates.



Import operation

Do you want to store all CA certificates on the eToken?

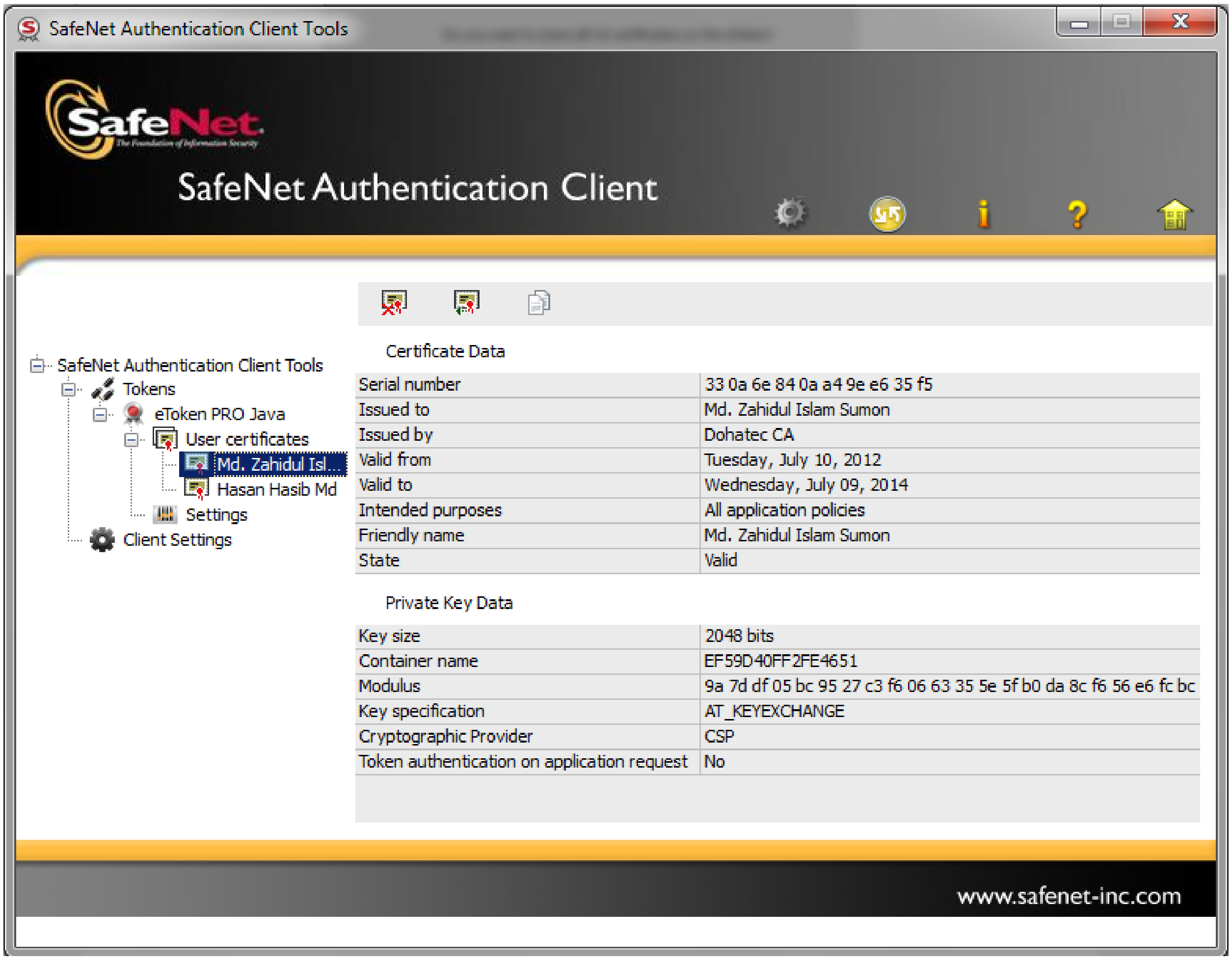
- A message confirming that the import was successful is displayed.



Import Certificate

Certificate imported successfully.

- The imported certificate can be checked under ‘User Certificates’.


SafeNet Authentication Client Tools
SafeNet
The Foundation of Information Security
SafeNet Authentication Client
SafeNet Authentication Client Tools
Tokens
eToken PRO Java
User certificates
Md. Zahidul Isl...
Hasan Hasib Md
Settings
Client Settings
www.safenet-inc.com

Certificate Data

Serial number	33 0a 6e 84 0a a4 9e e6 35 f5
Issued to	Md. Zahidul Islam Sumon
Issued by	Dohatec CA
Valid from	Tuesday, July 10, 2012
Valid to	Wednesday, July 09, 2014
Intended purposes	All application policies
Friendly name	Md. Zahidul Islam Sumon
State	Valid

Private Key Data

Key size	2048 bits
Container name	EF59D40FF2FE4651
Modulus	9a 7d df 05 bc 95 27 c3 f6 06 63 35 5e 5f b0 da 8c f6 56 e6 fc bc
Key specification	AT_KEYEXCHANGE
Cryptographic Provider	CSP
Token authentication on application request	No