

U S E R G U I D E



TATA CONSULTANCY SERVICES

Certificate Export/Import to E-token Pro (72K) Java

FOR USERS OF E-TOKENS

[VERSION 1.0]

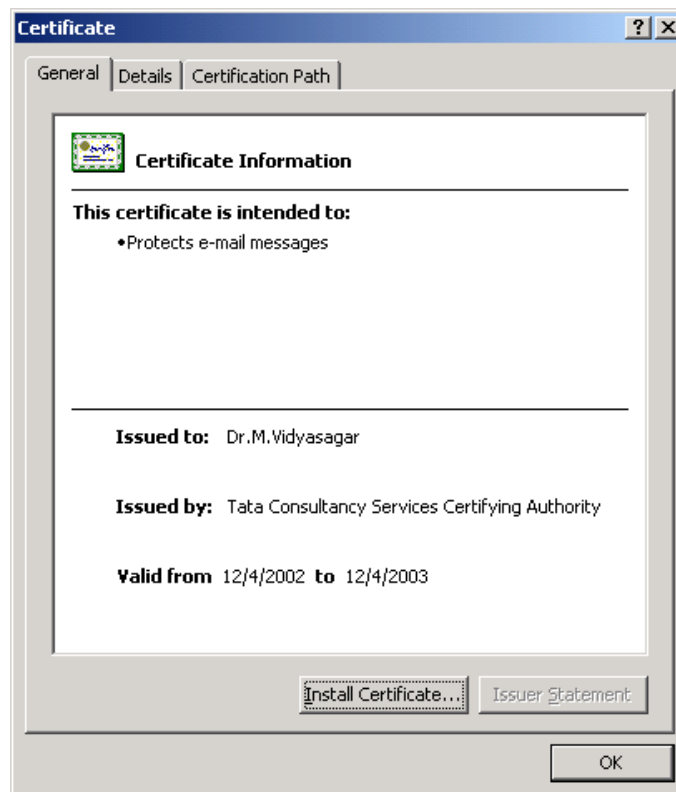
CONTENTS

1	DIGITAL CERTIFICATES	3
2	PKCS #12 FILES	6
2.1	Exporting a PKCS#12 File from the Browser	7
2.2	Importing PKCS #12 File onto the E-token.....	13

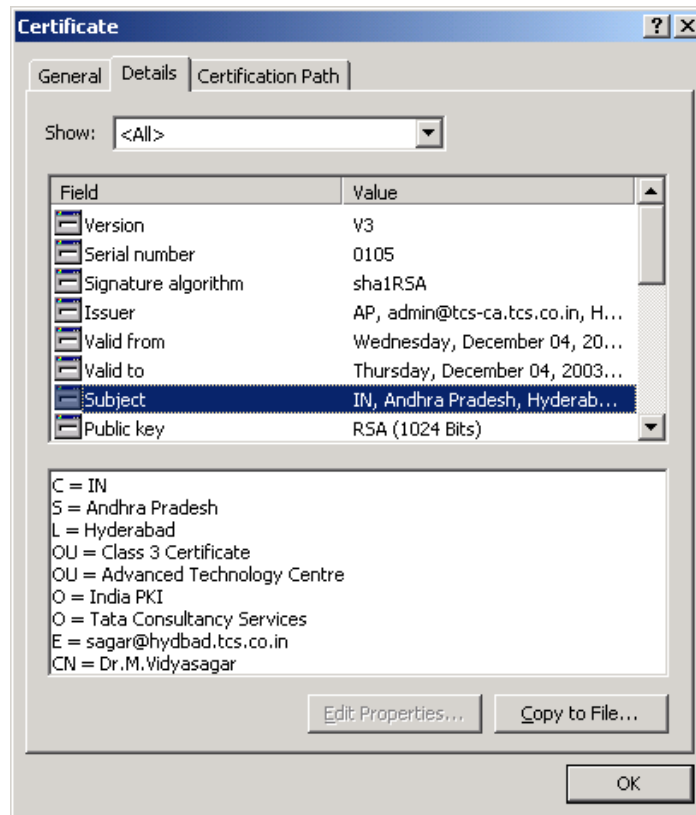
1 DIGITAL CERTIFICATES

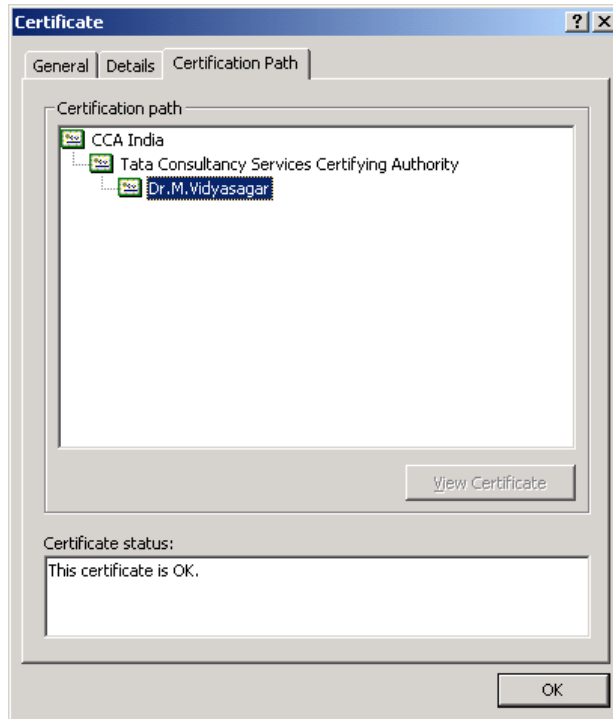
Certificates issued by TCS-CA are in X.509 v3 format. In Microsoft windows machines, these are recognized by the extension '.cer'.

To view a certificate, simply double click the .cer file.



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





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

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

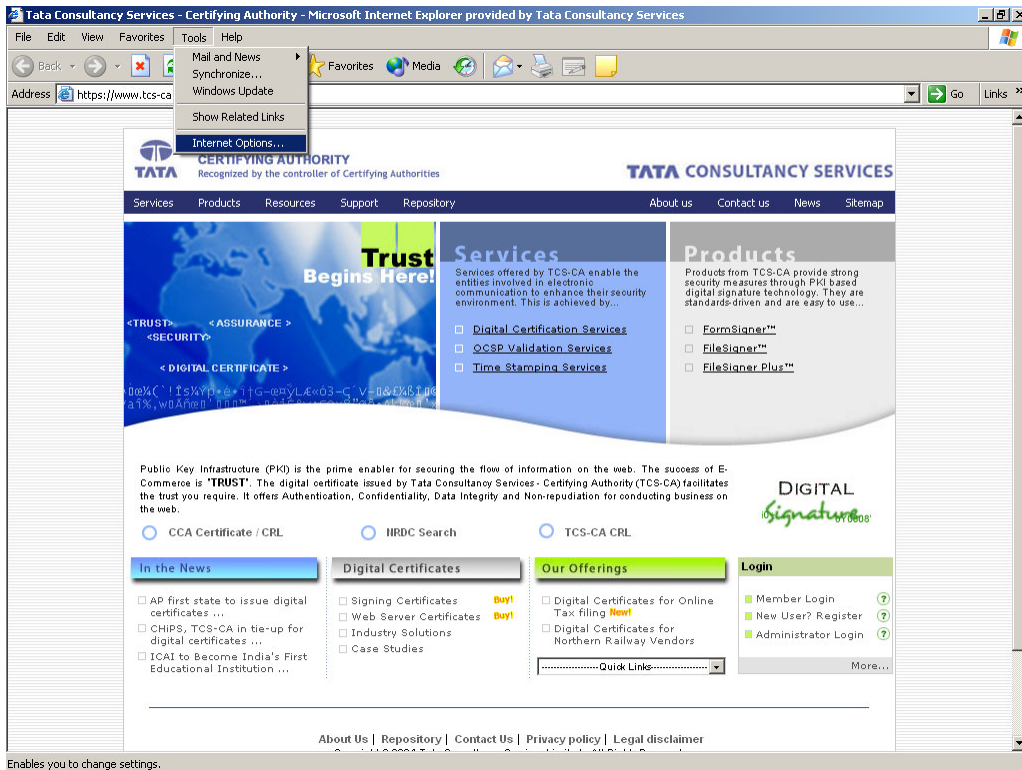
2 PKCS #12 FILES

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'

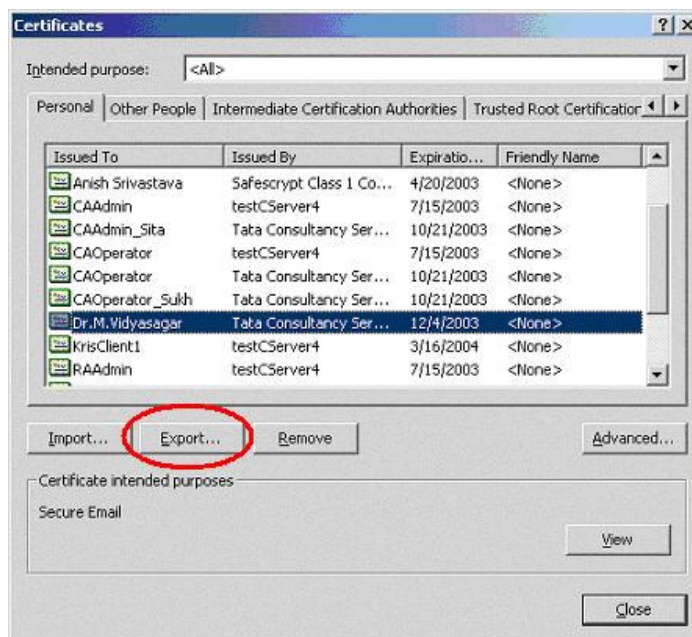
2.1 EXPORTING A PKCS#12 FILE FROM THE BROWSER



- 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.



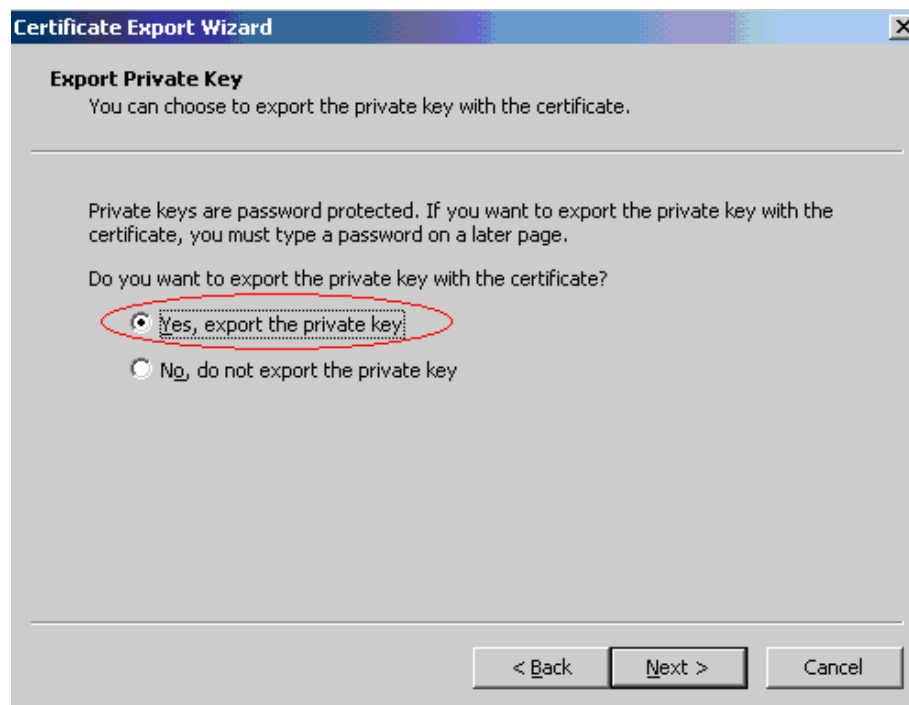
- Choose the certificate to be exported and click on the export tab.



- Click Next to the dialog to continue



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



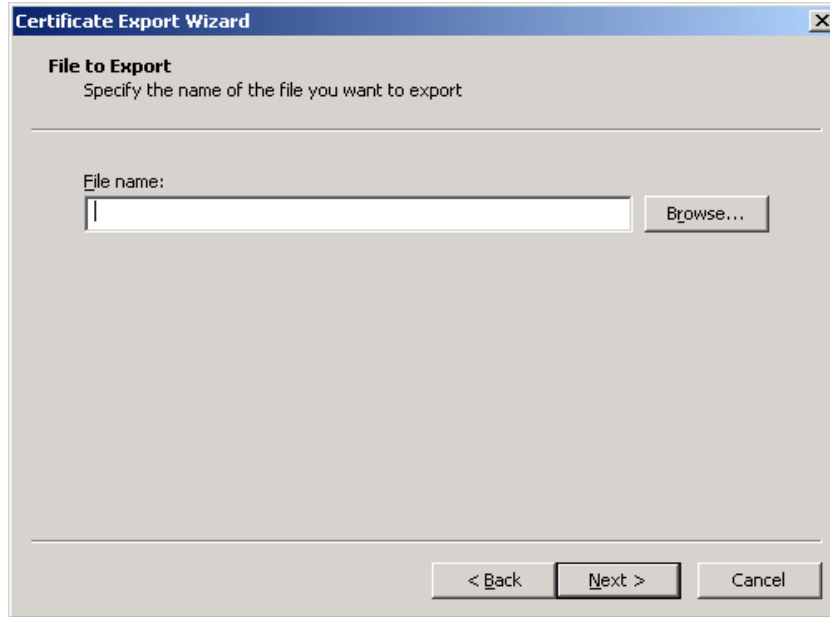
- Select the box indicated to include the CA certificate also with the Subscriber's certificate and Click 'Next'



- 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'



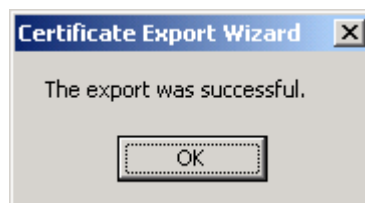
- Click Finish to export the private key and the certificates.



- 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 E-TOKEN

GETTING STARTED

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

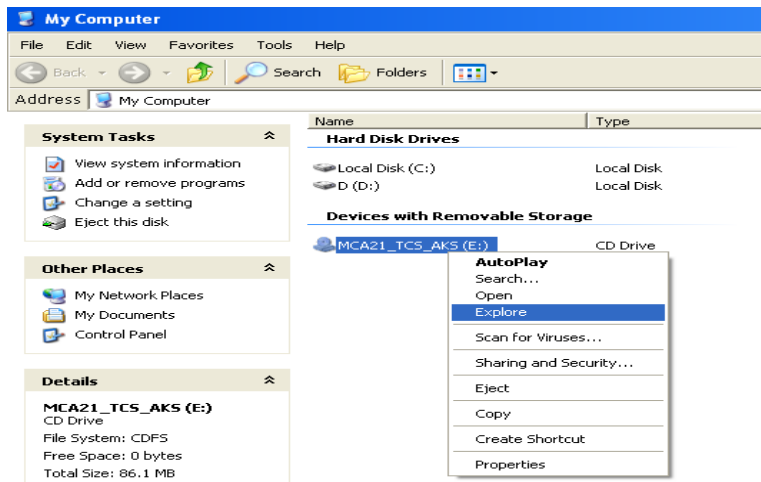
- USB Token (Aladdin E-Token pro Java)
- Installation CD contains:
 - USB Drivers

Note:

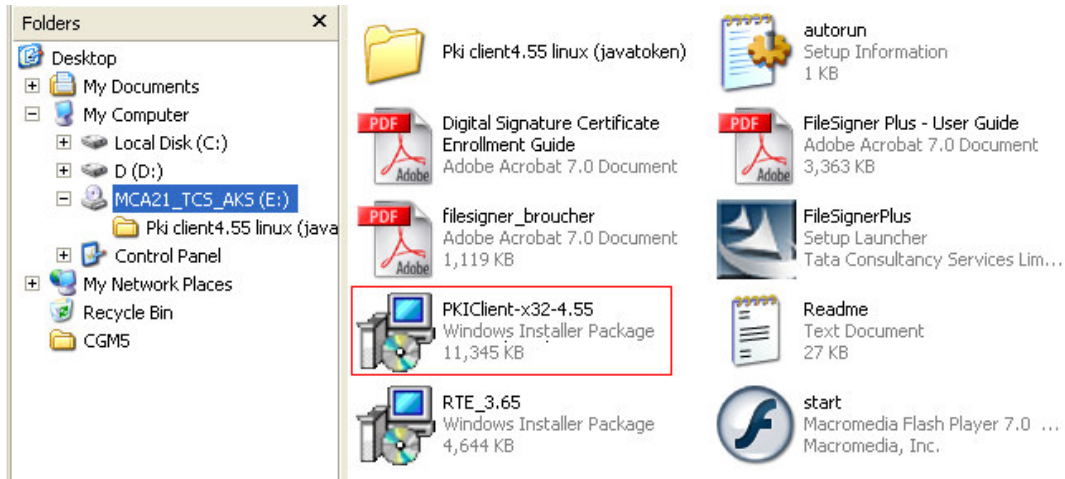
- *Use the Installation CD to install the USB Token driver.*
- *Ensure the following before installing the USB token driver.*

- ✓ System Requirement:
 - Operating System: Windows 2000, XP
 - Browser: Internet Explorer 5.5 and above
- ✓ You should have the Administrator privileges for installing the USB Token Driver.

1. To install E-Token Pro (72K) Java drivers, insert the CD and right click on the CD drive in 'My Computer' to select the option 'Explore'.

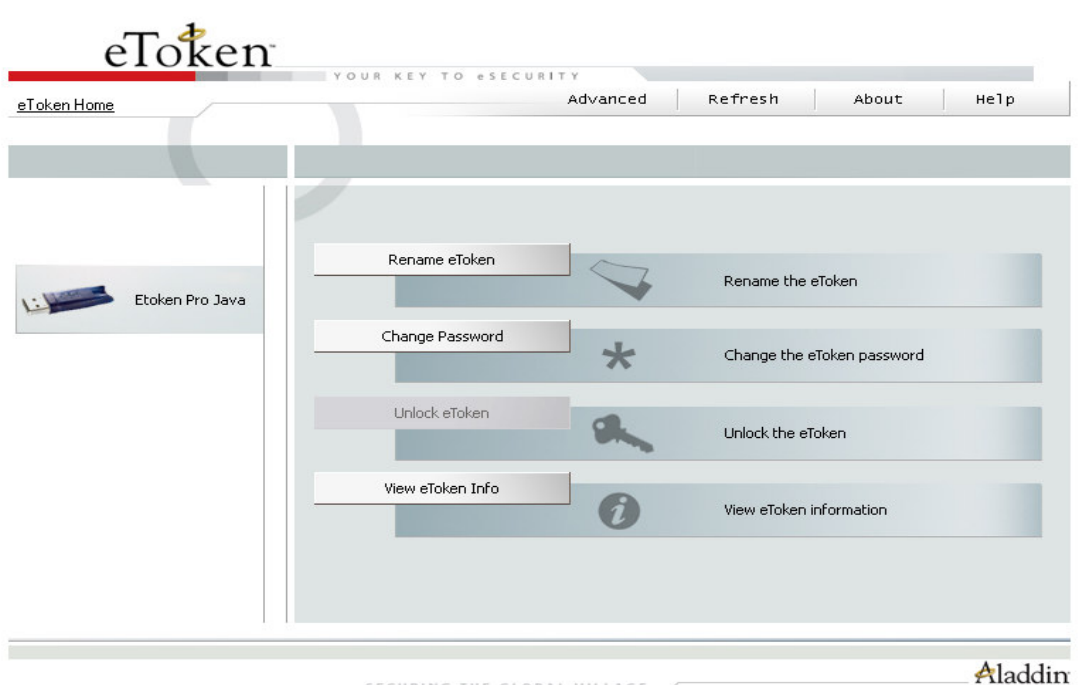


2. Click on the Windows Installer Package named '**PKIClient-x32-4.55**', accept the License Agreement and proceed with installation.




3. Insert the E-token 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 click on "E-Token Properties" with your E-Token inserted, the following screen is displayed.



Changing the E-Token Password:

All E-Tokens are configured at manufacture with the factory default password. This password is "1234567890". Click "Change password" on the E-Token Properties screen and the following E-Token Properties dialog is displayed:



The screenshot shows a Java dialog window titled "Change Password: eToken PRO Java". The dialog has a header with the text "Change Password" and the "eToken" logo. Below the header, there are three input fields: "Current eToken Password:", "New eToken Password:", and "Confirm New eToken Password:". To the right of the "Confirm New eToken Password" field is a progress indicator showing "0%". Below the input fields, there is a text box that reads: "Secure passwords are at least 8 characters long and include upper and lower case letters, punctuation marks, and numbers in random order." At the bottom of the dialog are "OK" and "Cancel" buttons.

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

Renaming the E-Token:

For additional convenience and ease of identification, the E-Token name can also be personalized. Click "Rename E-Token" on the E-Token Properties screen. Since renaming the E-Token requires the E-Token password, the following dialog is displayed:

Give the Password for the eToken and click "OK"



- Enter the new E-token name in the E-token name field and click on "OK" to set the E-token name.



- Click "OK" and in the E-Token Properties window the new E-Token name is displayed

The screenshot shows the eToken PKI Client interface. On the left, a tree view shows 'eToken PKI Client' expanded to 'Tokens & Readers', with 'Joe E-token' selected. The main window displays the properties for 'Joe E-token' under the 'Log On to eToken' tab. The 'Name' field is circled in red.

Initialize eToken	Log On to eToken	Import Certificate
Name	Joe E-token	
eToken category	Hardware	
Reader name	AKS ifdh 0	
Serial number	0x003bdeb0	
Total memory capacity	73728	
eToken card free space	32767	
Hardware version	4.29	
Firmware version	1.0	
Card ID	00 3b de b0	
Product name	eToken PRO Java 72K 05755	
Model	Token 4.29.1.1 1.0.37	
Card Type	Java Card	
OS version	eToken Java Applet 1.0.37	
Color	Blue	
Supported key size	2048	
User password	Present	
User password retries remaining	15	
Maximum user password retries	15	
Administrator password	Absent	

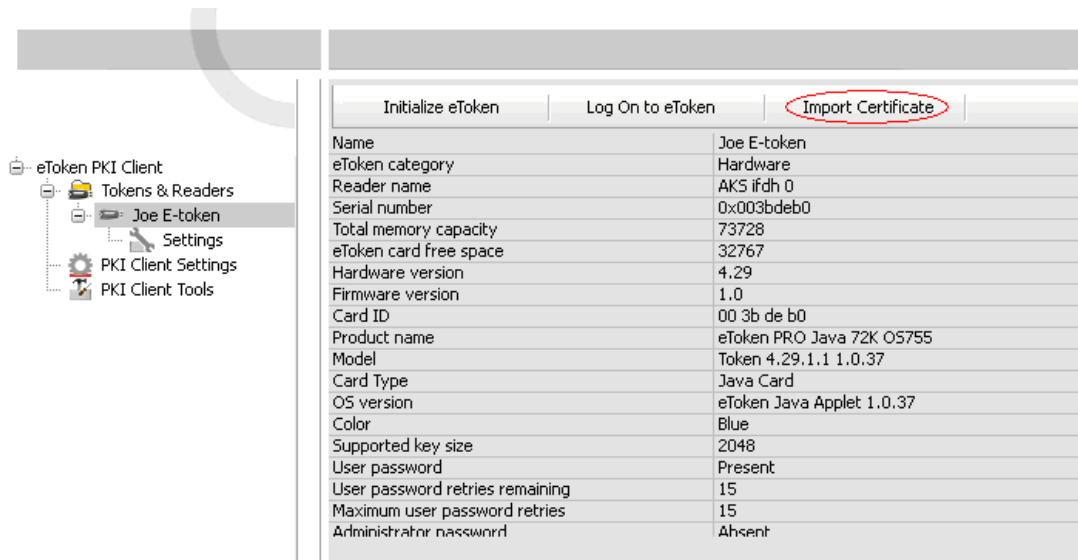
Import Procedure:

Select the 'Advanced' option on the E-token properties screen and select the option 'Logon to the E-token' and provide the E-token password to login and import the certificate.

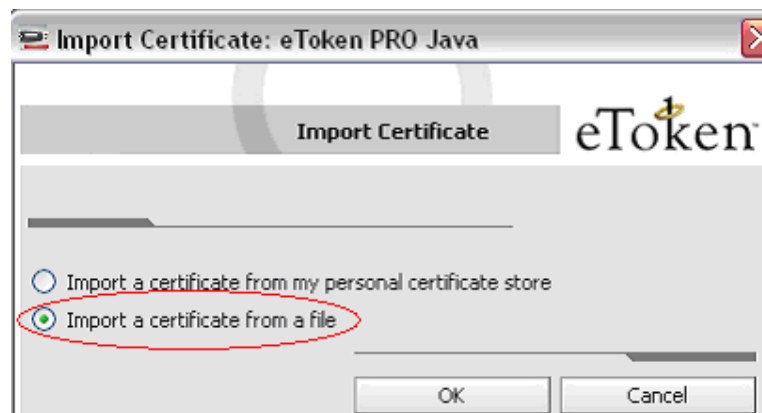
The screenshot shows the eToken PKI Client interface with the 'Log On to eToken' tab selected in the main window. The 'Log On to eToken' tab is circled in red. The left sidebar shows 'eToken PKI Client' expanded to 'Tokens & Readers', with 'Joe E-token' selected.

Initialize eToken	Log On to eToken	Import Certificate
Name	Joe E-token	
eToken category	Hardware	
Reader name	AKS ifdh 0	
Serial number	0x003bdeb0	
Total memory capacity	73728	
eToken card free space	32767	
Hardware version	4.29	
Firmware version	1.0	
Card ID	00 3b de b0	
Product name	eToken PRO Java 72K 05755	
Model	Token 4.29.1.1 1.0.37	
Card Type	Java Card	
OS version	eToken Java Applet 1.0.37	
Color	Blue	
Supported key size	2048	
User password	Present	
User password retries remaining	15	
Maximum user password retries	15	
Administrator password	Absent	

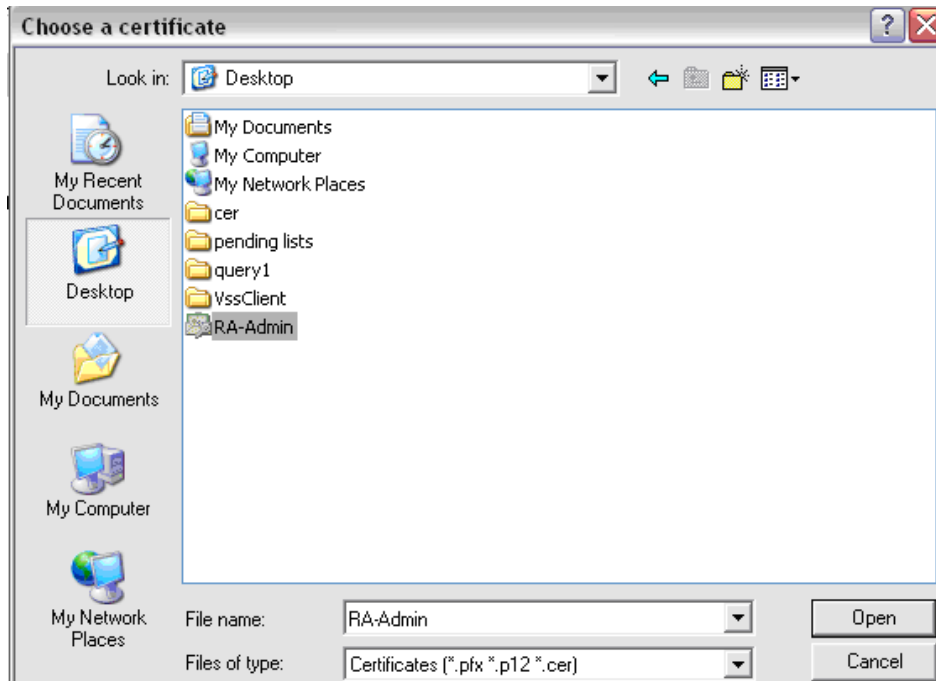
- Click "Import certificate" to import your certificate from ".PFX file" from a location on your Computer.



- Select "Import certificate from the file" and click "OK".



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

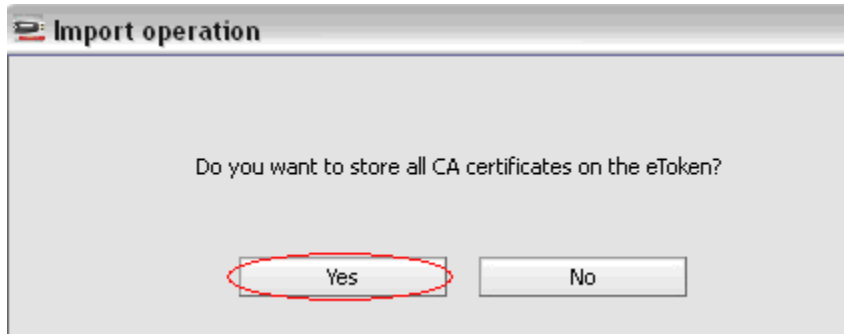


- A prompt for Password for the private key appears. Give the password that you had set to protect the file, while exporting the certificate and click "OK"

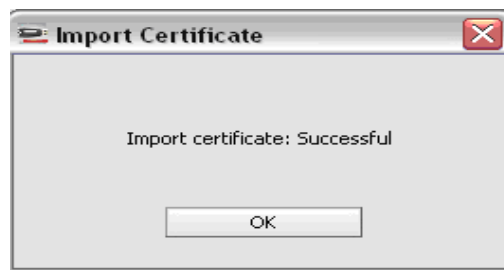


A certificate that is stored on the computer may be part of a hierarchical structure with more than one Certificate in the chain up to the Root CA. Importing a CA Chain takes the CA certificate and the complete CA Chain up to the root certificate that is stored on the computer and places it on the E-Token.

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



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



- The imported certificate can be checked under 'User Certificates' along with the root certificates.





TATA
TATA CONSULTANCY SERVICES

CONTACT US

Tata Consultancy Services Limited
[Certifying Authority - PKI Services]
Advanced Technology Centre
Deccanpark, 1 - Software Units Layout
Madhapur, Hyderabad - 500 081.
Phno: 040 – 6667 3524 / 25 / 26.

✉ helpdesk@tcs-ca.tcs.co.in

🌐 <http://www.tcs.com>



TATA
TATA CONSULTANCY SERVICES
