



www.charteredinfo.com

Certificate Import to Aladdin eToken

CONTACT:

CHARTERED INFORMATION SYSTEMS PVT. LTD.

"Chartered House",

West of Lata Mangeshkar Musical Park,

Bhandara Road, NAGPUR - 440 008

Tel: +91 (0712) 663 8888, 92252 45088

digitalsognature@charteredinfo.com

www.charteredinfo.com

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 eToken)
- Installation CD. This contains:
 - USB Drivers
 - Mozilla Firefox
 - TCS FileSigner Plus Evaluation Copy

Note:

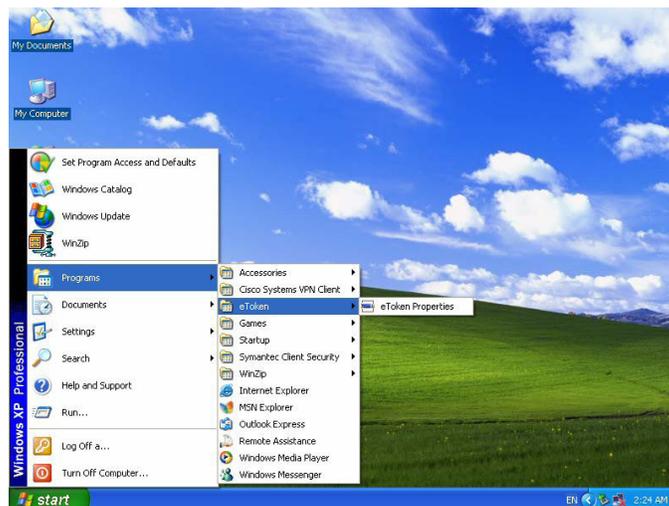
- *Use the Installation CD to install the USB Token driver.*
- *Ensure the following before installing the USB token driver.*

- ✓ 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

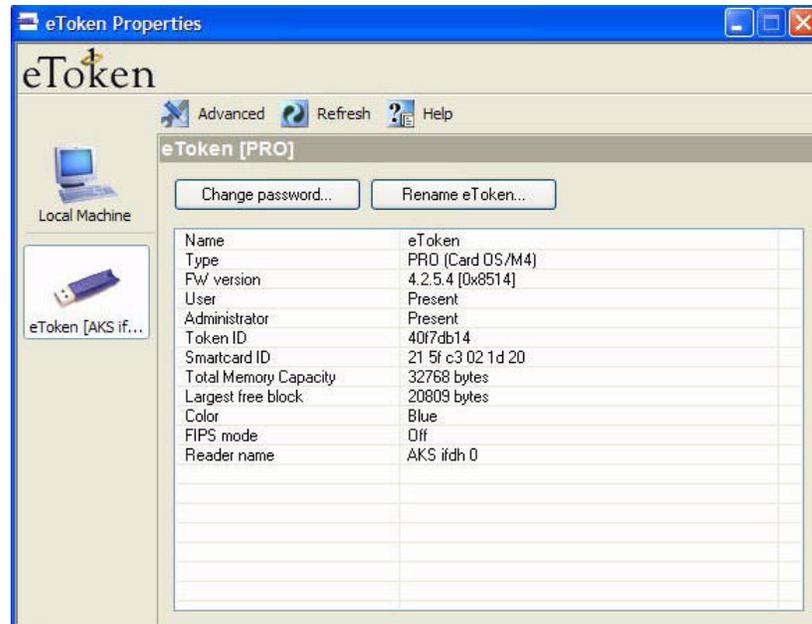
USING ALADDIN ETOKEN

To install the eToken:

1. Insert the CD into the CD drive of your computer.
 2. To install eToken driver click on **etoken_driver_aladin.msi** Windows Installer Package. Accept the License Agreement and proceed with installation.
 3. Insert the USB Token in the USB port of the computer, if prompted
 4. Restart the computer after the installation is complete.
- You can now see the eToken Properties from the Start Menu by selecting Programs> eToken> eToken Properties



Click "eToken Properties" and with your eToken inserted, the following screen is displayed:



CHANGING THE ETOKEN PASSWORD

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



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 eTOKEN

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

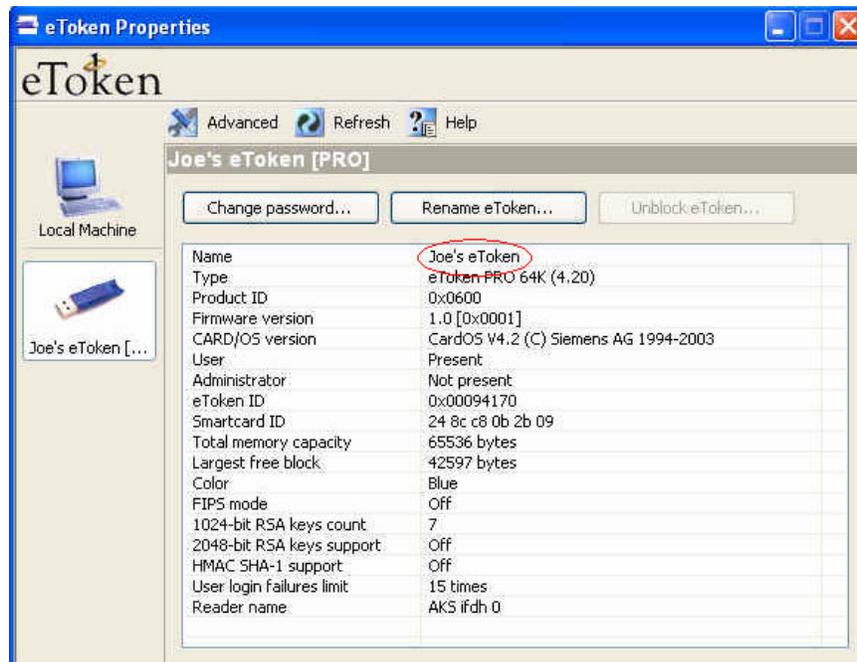
Give the Password for the eToken and click "OK"



Enter the new eToken name in the eToken Name field and click "OK" to set the eToken Name.



Click "OK" and in the eToken Properties window the new eToken name is displayed.



IMPORTING THE CERTIFICATE INTO ETOKEN

To import the Certificate, you first need to export the certificate from the IE Browser onto the Desktop and then import it into the eToken.

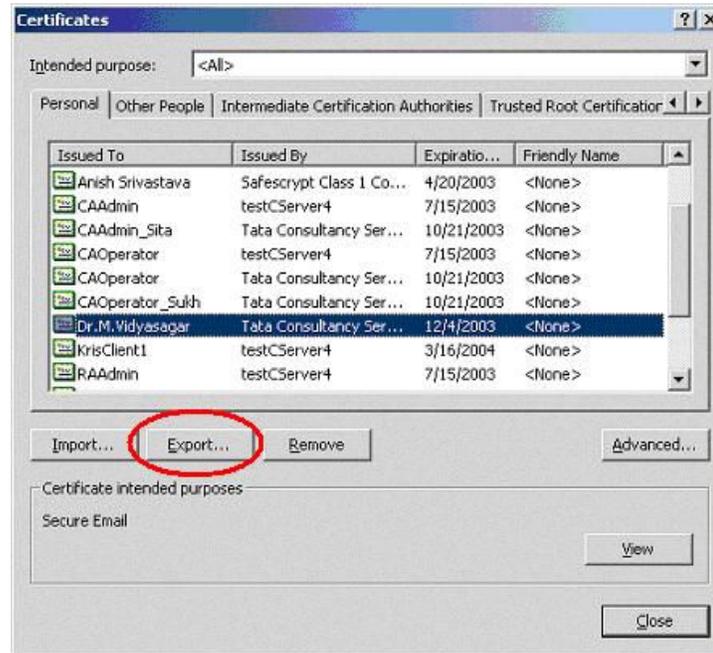
EXPORTING THE CERTIFICATE

Exporting the Digital Certificate from the browser and maintaining its backup as a '.pfx' file is essential since, at any point of time if your certificate gets deleted from the browser or token or if you format your system, you can always import it again.

For exporting your Certificate that has been downloaded in your browser, Open the IE Browser and follow the path

“ Tools>Internet Options>Content>Certificate>Personal” tab.

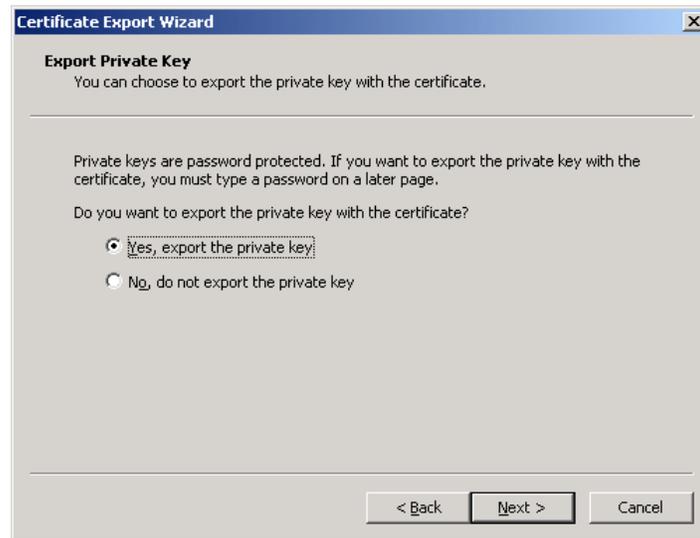
Choose the certificate to be exported and click on the export tab.



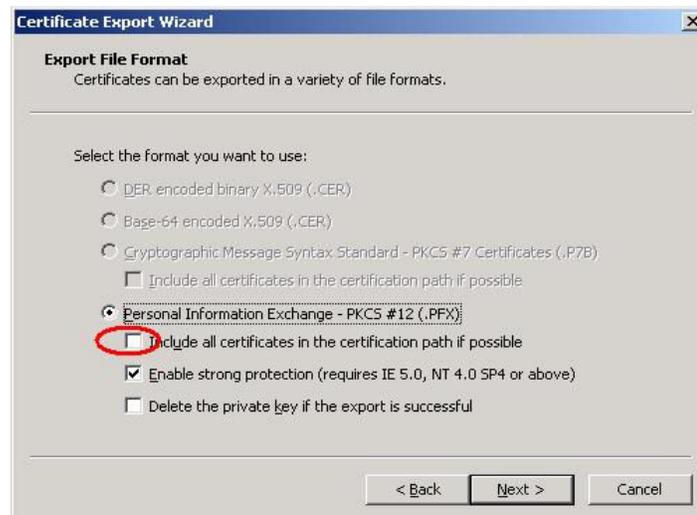
Click Next to the dialog to continue



choose the option 'Yes', export the private key' 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. Ensure that you remember this password since you will be needing it while importing the certificate at a later point of time.



The image shows a screenshot of the 'Certificate Export Wizard' dialog box, specifically the 'Password' step. The title bar reads 'Certificate Export Wizard' with a close button (X) on the right. The main heading is 'Password' with a sub-instruction: 'To maintain security, you must protect the private key by using a password.' Below this, the text says 'Type and confirm a password.' There are two text input fields: the first is labeled 'Password:' and the second is labeled 'Confirm password:'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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



The image shows a screenshot of the 'Certificate Export Wizard' dialog box, specifically the 'File to Export' step. The title bar reads 'Certificate Export Wizard' with a close button (X) on the right. The main heading is 'File to Export' with a sub-instruction: 'Specify the name of the file you want to export'. Below this, there is a text input field labeled 'File name:' and a 'Browse...' button to its right. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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



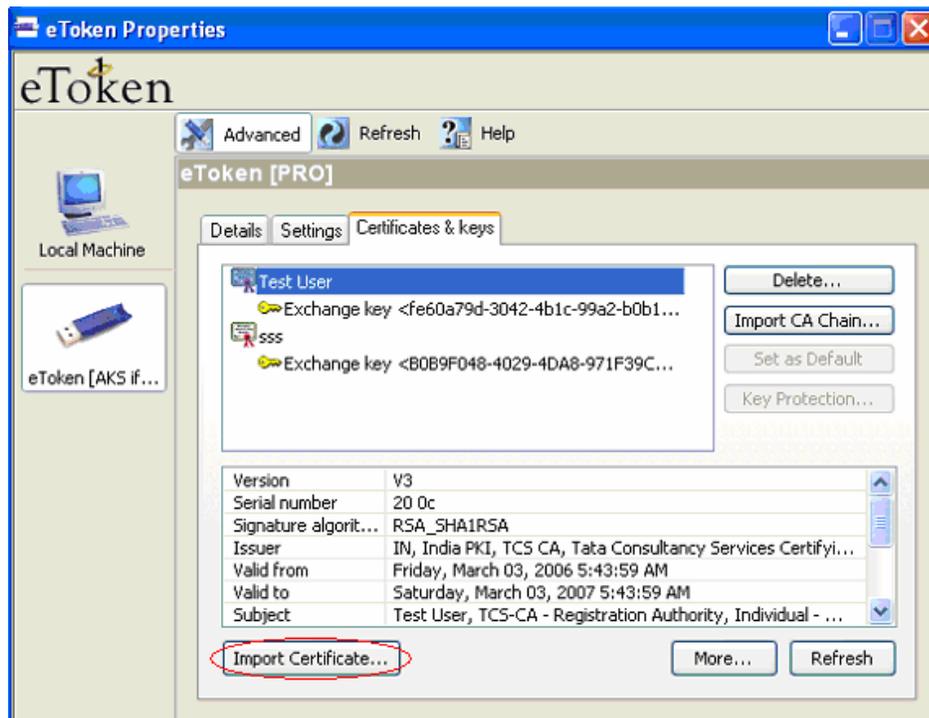
A message will be shown indicating the successful completion of the export.



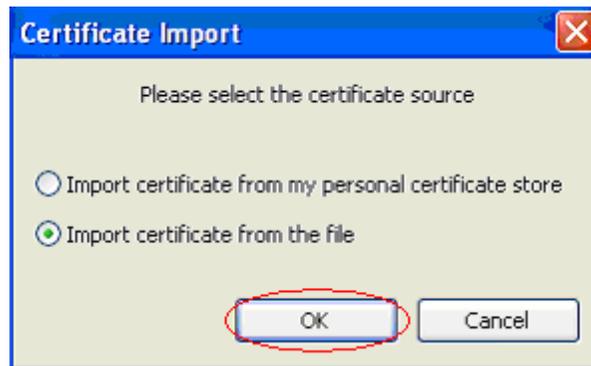
IMPORTING THE CERTIFICATE INTO ETOKEN

From the Start Menu by selecting
Programs> eToken> eToken Properties>Advanced>Certificate & Keys

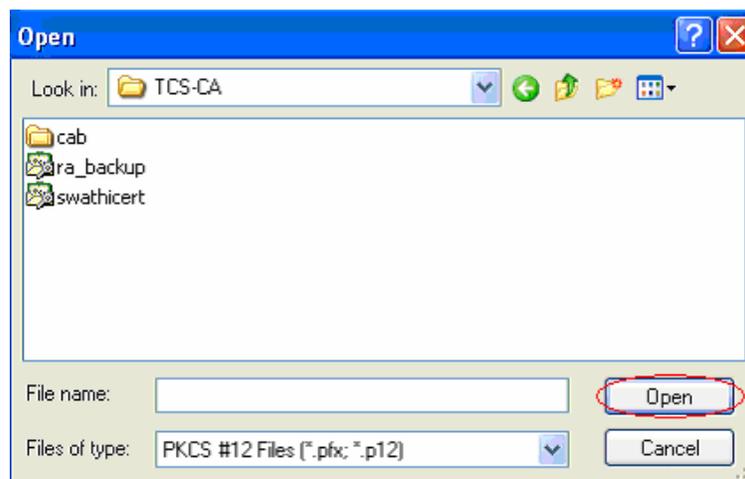
The following Dialogue box appears. Click 'Import Certificate'



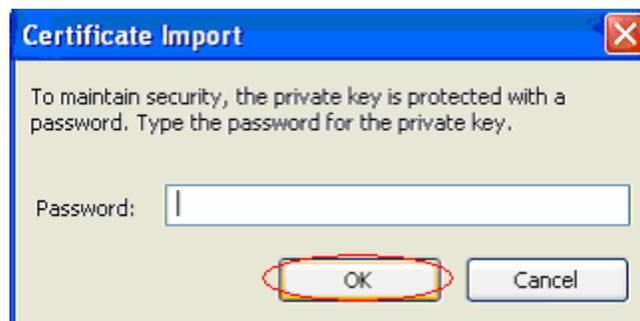
If the import is from a file, which has already been exported to a particular location on your computer, then select "Import certificate from the file" and click "OK".



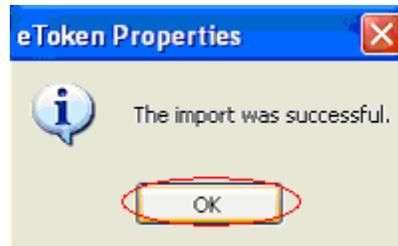
Select the path of the ". pfx" file and click "Open".



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



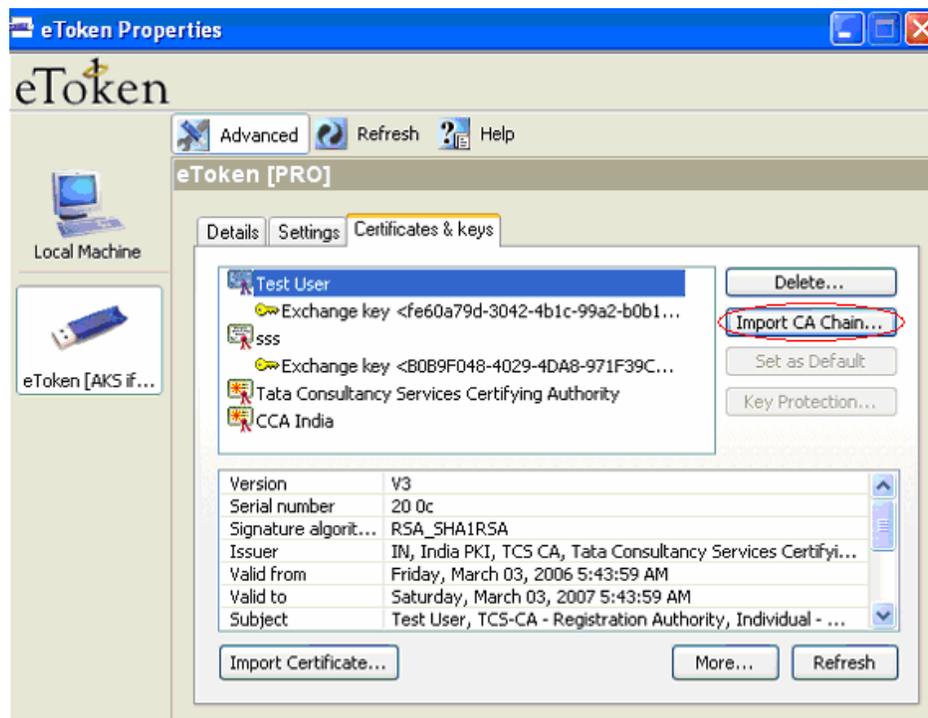
A confirmation message is displayed if the import is successful.



IMPORTING THE CA CHAIN

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 "Import CA Chain" button is clicked, the CA Chain is imported onto the eToken and displayed in the certificate and key list window:



A message confirming the import was successful is displayed

