TATA CONSULTANCY SERVICES

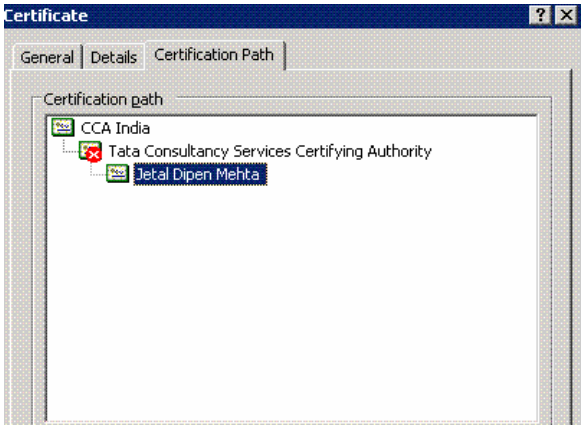
TCS.Beyond the obvious.

User Guide for Installing TCS-CA Trust Chain.

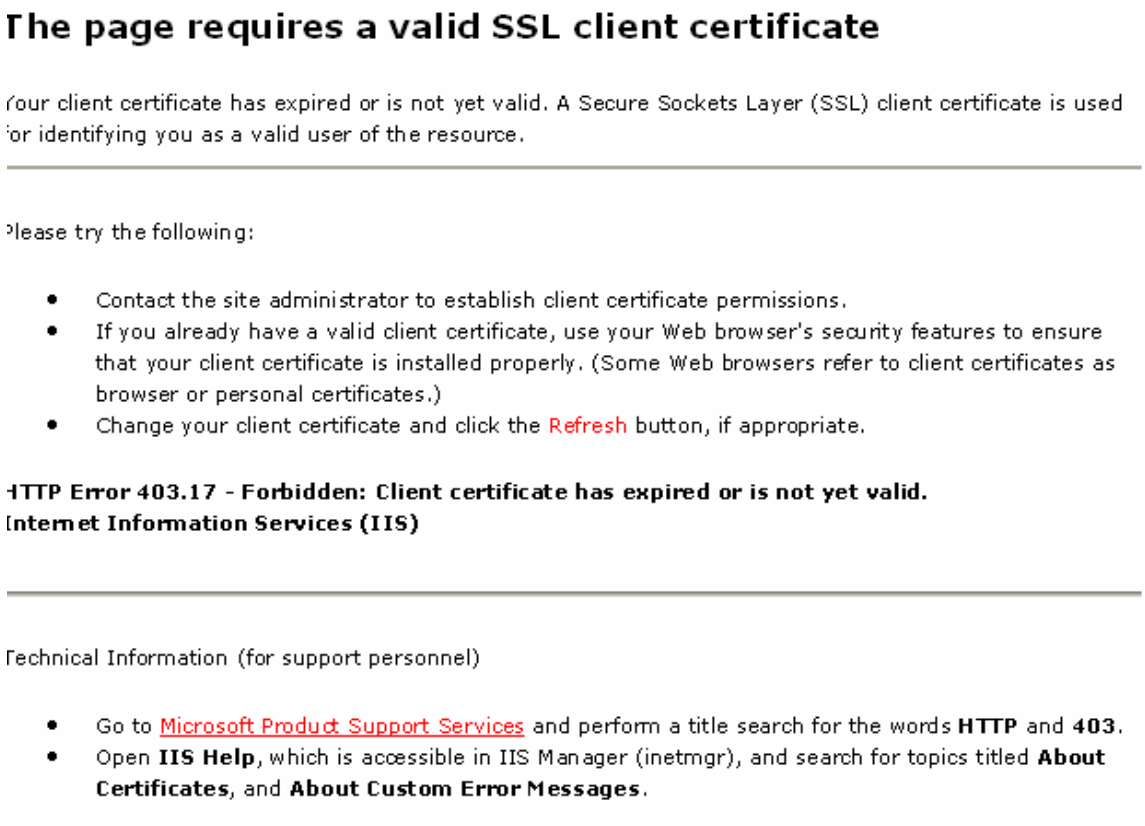
ABOUT THE DOCUMENT

This document describes the procedure to install TCS-CA Trust Chain for the subscribers to whom Digital Signature Certificates were issued during the period Tuesday, March 28, 2006 to Saturday, July 04, 2009 and who have encountered an error "Certificate has expired or not yet valid" or "The page requires a valid SSL client certificate".

ERROR SCENARIO-I



ERROR SCENARIO-II



The page requires a valid SSL client certificate

Your client certificate has expired or is not yet valid. A Secure Sockets Layer (SSL) client certificate is used for identifying you as a valid user of the resource.

Please try the following:

- Contact the site administrator to establish client certificate permissions.
- If you already have a valid client certificate, use your Web browser's security features to ensure that your client certificate is installed properly. (Some Web browsers refer to client certificates as browser or personal certificates.)
- Change your client certificate and click the Refresh button, if appropriate.

HTTP Error 403.17 - Forbidden: Client certificate has expired or is not yet valid.
Internet Information Services (IIS)

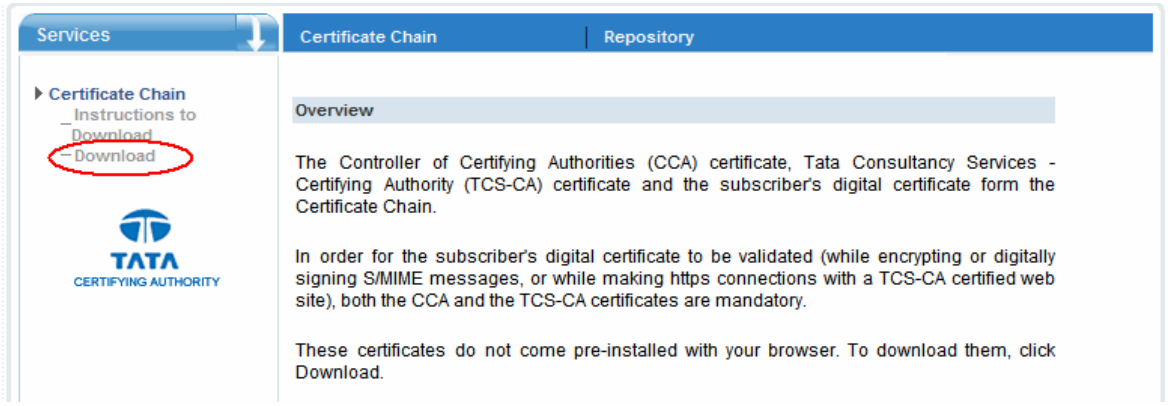
Technical Information (for support personnel)

- Go to Microsoft Product Support Services and perform a title search for the words **HTTP** and **403**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **About Certificates**, and **About Custom Error Messages**.

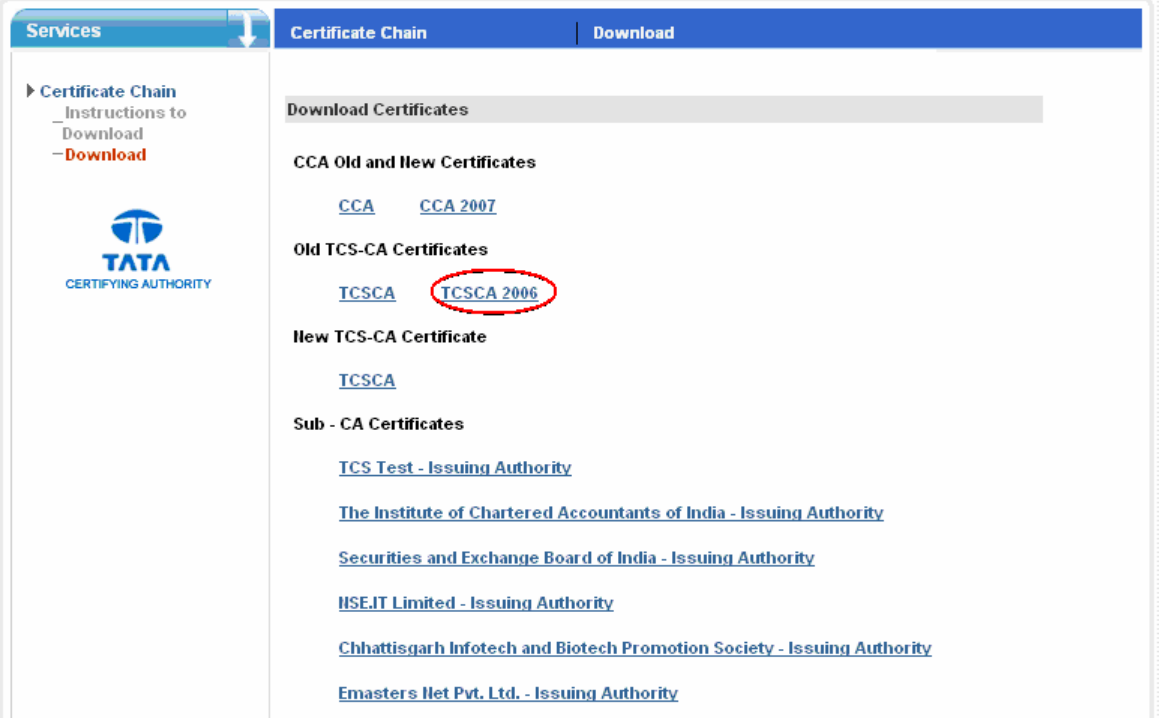
GETTING STARTED

1) Log on to https://www.tcs-ca.tcs.co.in
2) Click on **Certificate Chain (TCS-CA & CCA).**

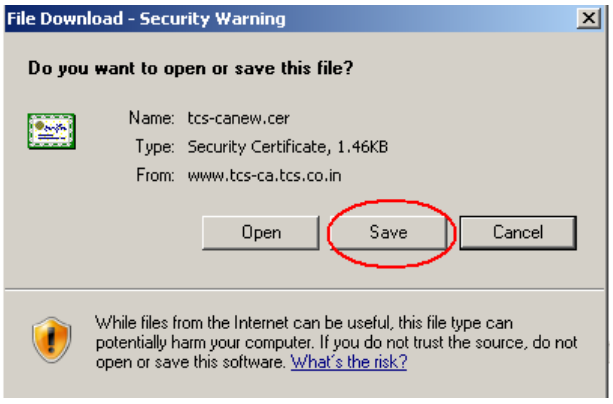
3) Click **Download**.



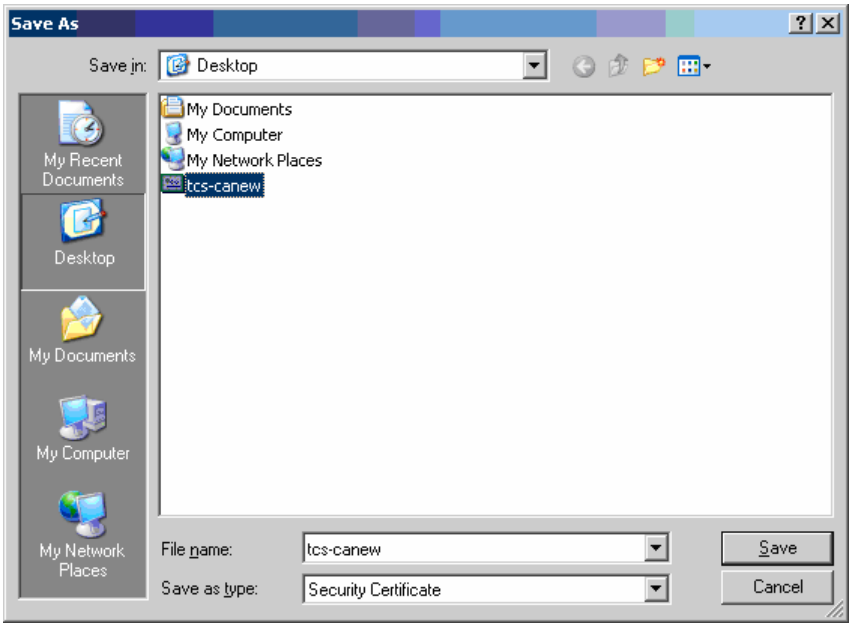
4) Click on **TCSCA 2006.**



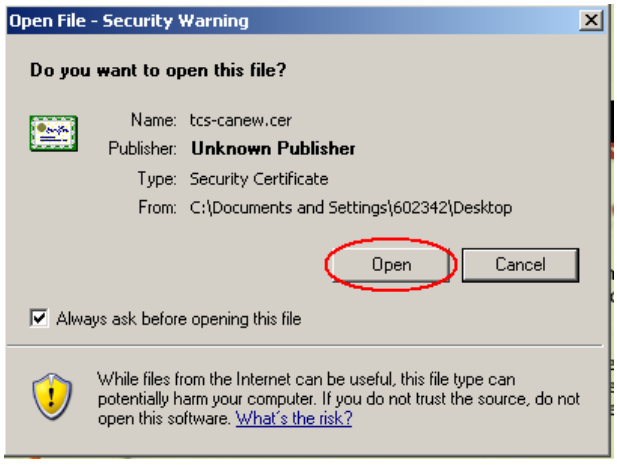
5) Click **Save** to save the tcs-canew.cer file on your system.



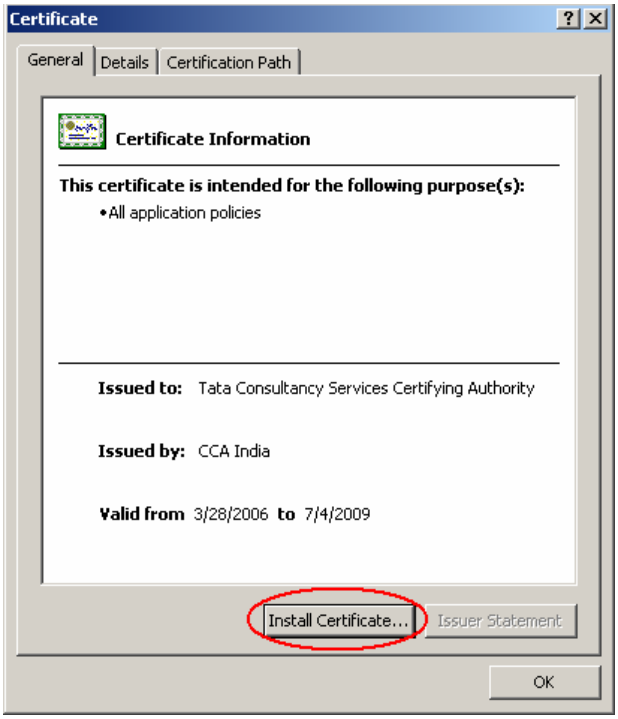
6) Save the Trust Chain on Desktop.



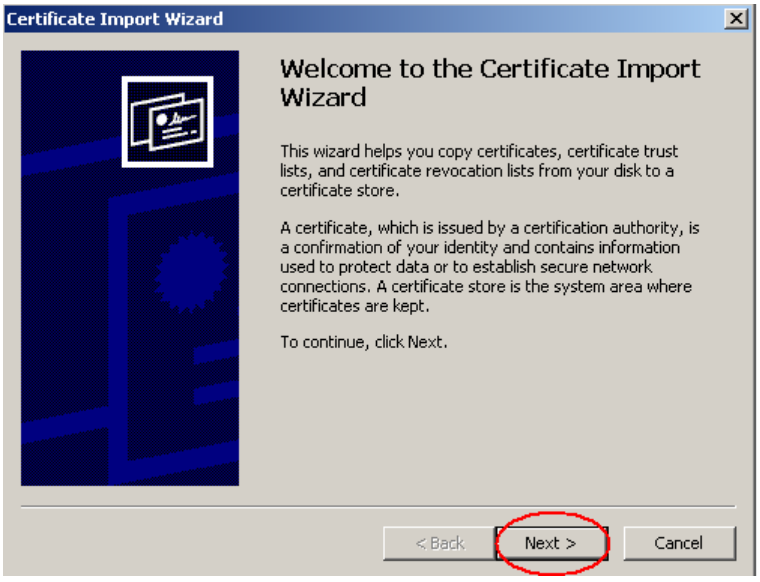
7) Double Click on the certificate and click **open**.



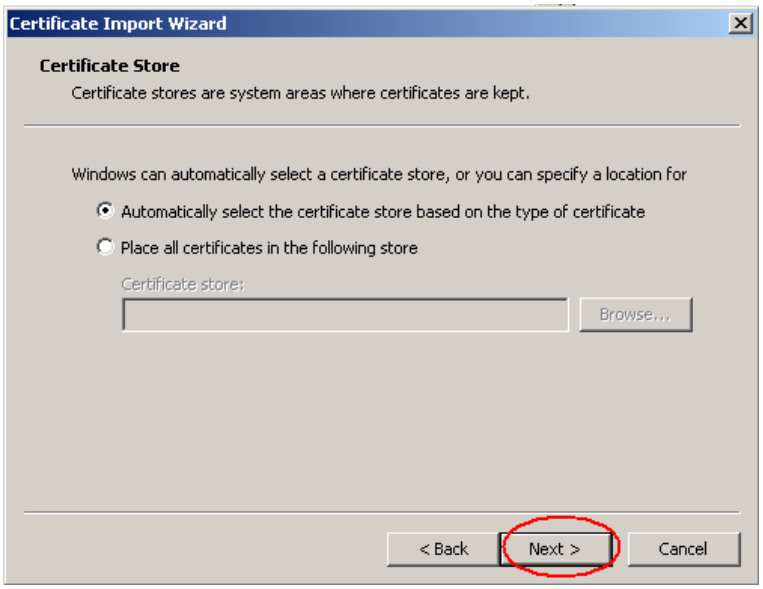
8) Click **Install Certificate**.



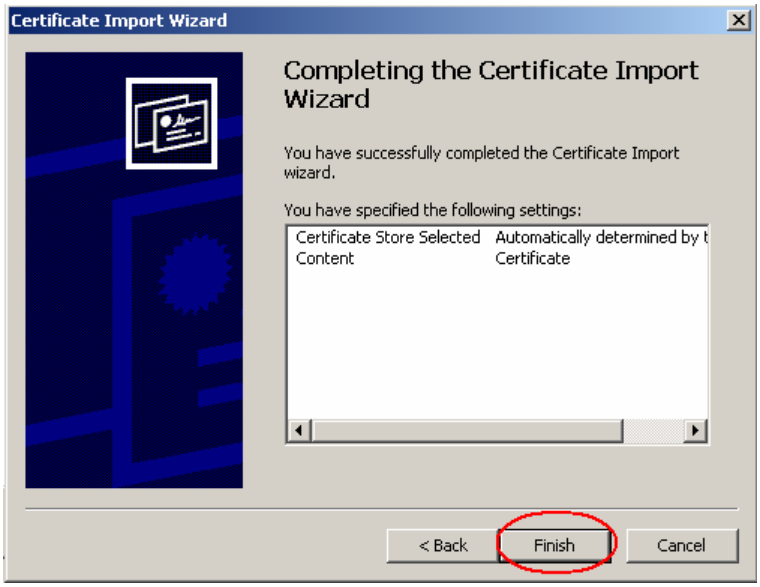
9) Click **Next**.



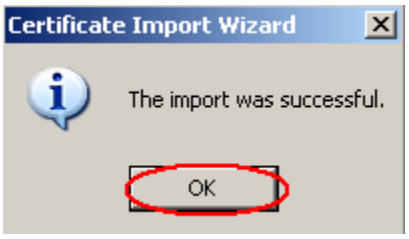
10) Select **"Automatically select the certificate store"** and Click **Next**.



11) Click **Finish** to complete the certificate import.

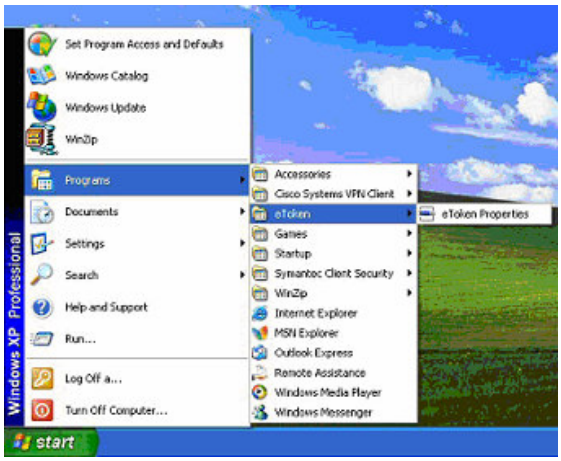


12) Click **OK** to successfully import the TCS-CA Trust Chain into your browser.

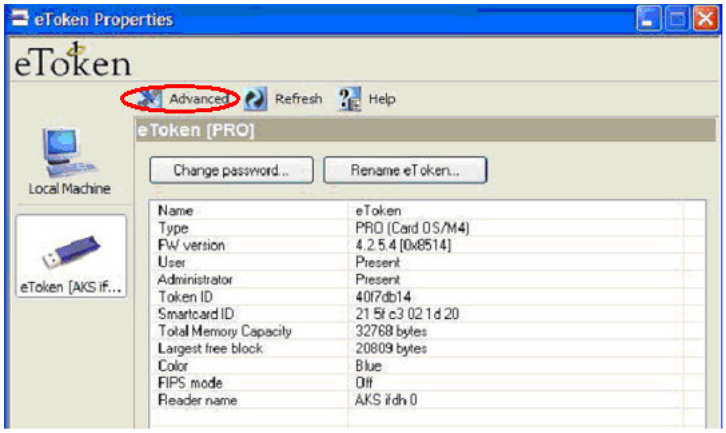


13) In case you have your personal Digital Signature Certificate along with the trust chain in your eToken. Kindly follow the below steps

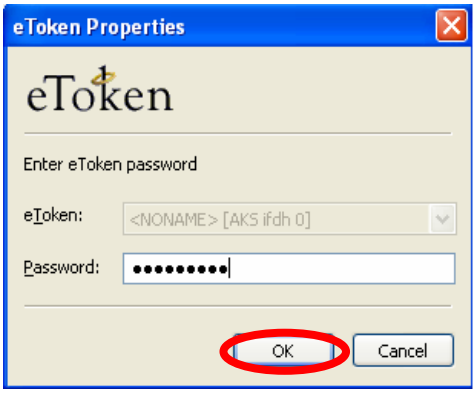
a) From the Start menu, select Programs >eToken >eToken Properties.



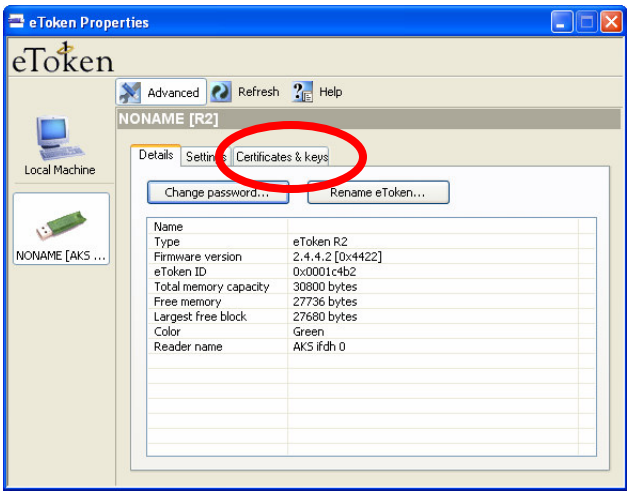
b) When you insert your eToken key, the following screen is displayed. Click the **Advanced** tab.



c) Provide your eToken password and click **OK**.

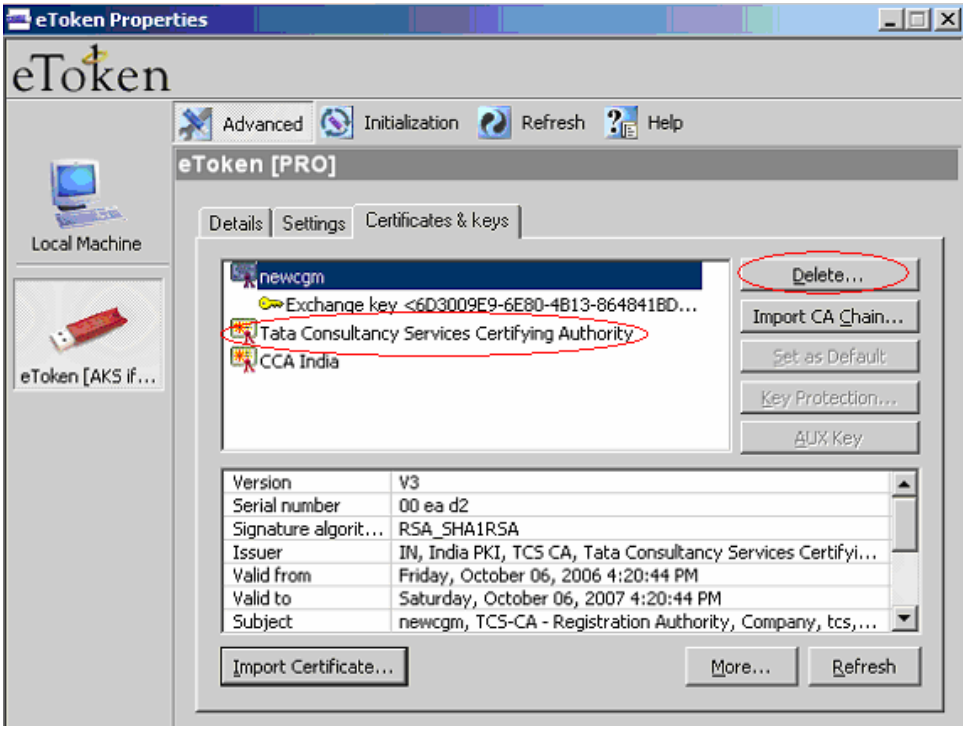


d) The following Dialog box appears. You can view the details of the eToken.



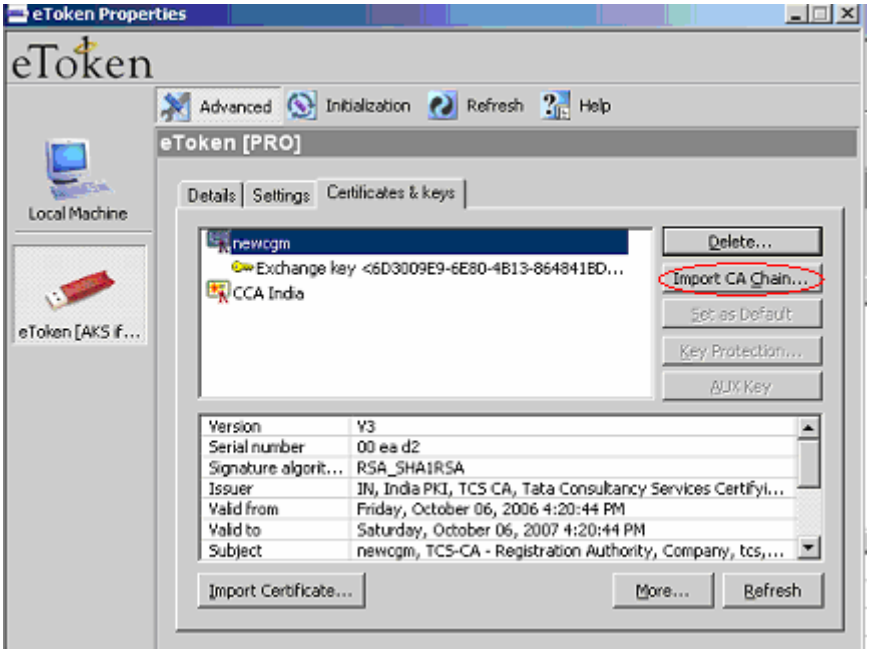
e) Click **Certificates & Keys**. You can view your Certificate, Key, and the details like Certificate serial number, Issuer details, Certificate validity etc.

f) Delete the old TCS-CA certificate which has expired **(Valid till 8th October 2007)** from the token.

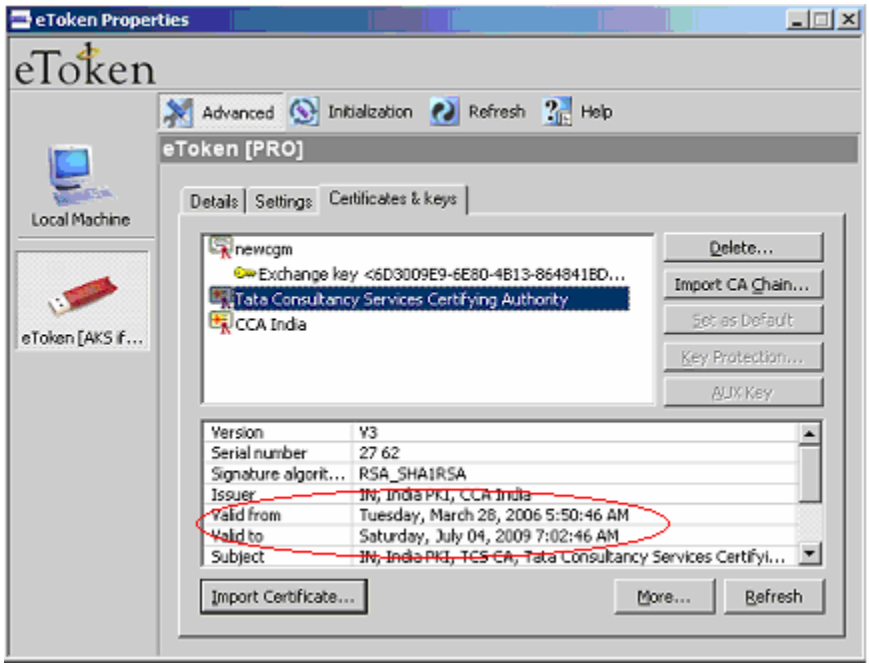


Please Note: Kindly ensure that you delete only "TCS-CA Root/Chain Certificate" and not end user certificate

g) Now click "Import CA Chain" to import new TCS-CA certificate into your eToken.



h) Confirm the validity of the imported TCS-CA certificate as per the below screenshot.



Please Note: The newly imported TCS-CA Root Certificate will be valid from Tuesday, March 28, 2006 to Saturday, July 04, 2009

CONTACT US

Tata Consultancy Services Limited
[Certifying Authority - PKI Services]
Advanced Technology Centre
deccanpark, 1 - Software Units Layout
Madhapur, Hyderabad - 500 081

✉ helpdesk@tcs-ca.tcs.co.in
💻 http://www.tcs.com

TATA CONSULTANCY SERVICES