

# Obtaining a digital signature certificate

This document is an extract from the book *Ecommerce - Legal Issues* authored by Rohas Nagpal. This book is available as courseware for the **Diploma in Cyber Law** and **PG Program in Cyber Law** conducted by Asian School of Cyber Laws



[www.asianlaws.org](http://www.asianlaws.org)



## 5. Obtaining a digital signature certificate

This chapter serves as a ready reference for the procedure of obtaining a digital signature certificate from a licenced Certifying Authority in India.

For the purposes of this chapter, the step by step procedure is outlined. The application for the certificate is made in the name of “Rohas Nagpal” to the Tata Consultancy Services Certifying Authority. A computer running Microsoft Windows XP operating system and Microsoft Internet Explorer 7 is used.

Where relevant, information obtained from the Tata Consultancy Services Certifying Authority website ([www.tcs-ca.tcs.co.in](http://www.tcs-ca.tcs.co.in)) has been quoted.

The steps followed to obtain the digital signature certificate are as under:

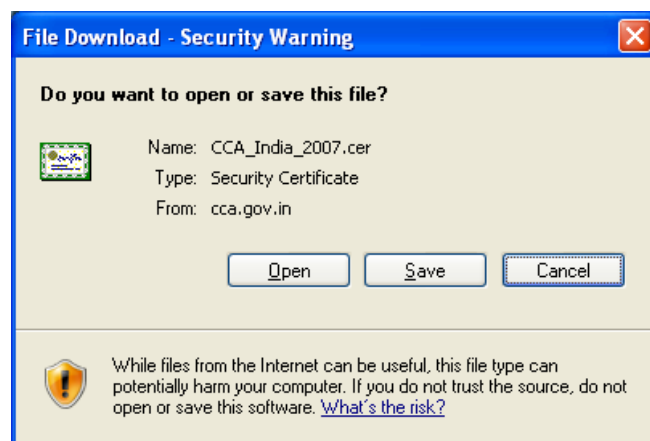
### 1. Downloading root certificate

Visit the website of the Controller of Certifying Authorities (CCA) at [www.cca.gov.in](http://www.cca.gov.in) to obtain the digital signature certificate of the CCA. This certificate must be installed on our computer before we begin the process to obtain our personal digital signature certificate. The detailed procedure for the same is outlined below:

- i. Click on “**Download 2007 Root Certificate**” image.



- ii. The following screen will open up. Click on “**Open**”



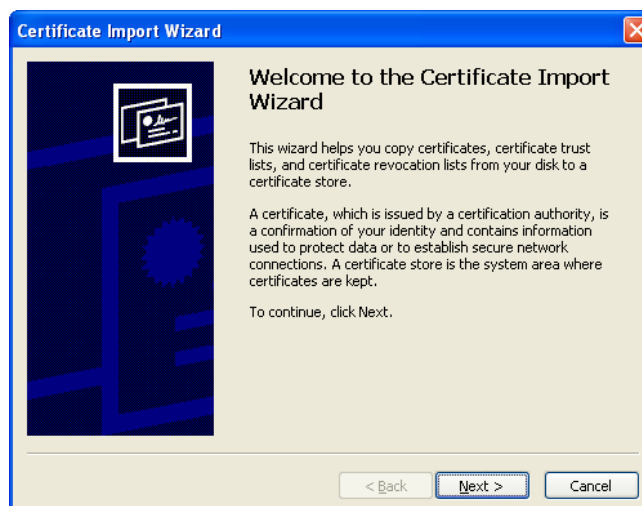
- iii. The following digital signature certificate will open up on your screen:



- iv. The certificate displays the message that:

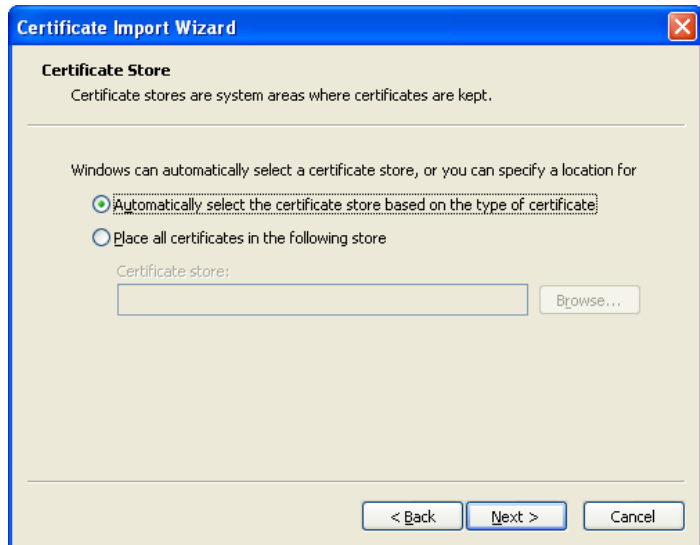
“This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store”.

The reason for this is that this certificate is not installed in the Microsoft Internet Explorer browser by default. We will manually need to do so. Click on “**Install Certificate**”. The following screen opens up:





- v. Click on “**Next**”. The following screen will open up. Again click on “**Next**”.



- vi. The following screen will open up. Click on “**Finish**”.



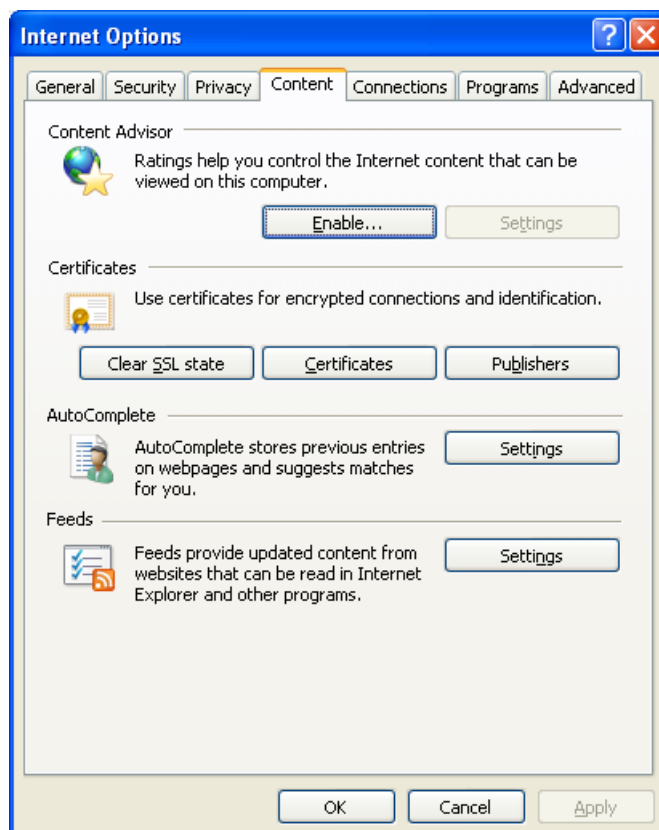
- vii. This is the final stage for installing the CCA certificate on our computer. It must be clearly understood that once this root certificate is installed in our browser, it becomes a trusted **root** certificate. All Certifying Authorities who are issued certificates by the CCA will automatically be trusted by our computer.
- viii. The following screen will open up. Click on “**Yes**”.



- ix. The screen below will open up. Click “OK”.

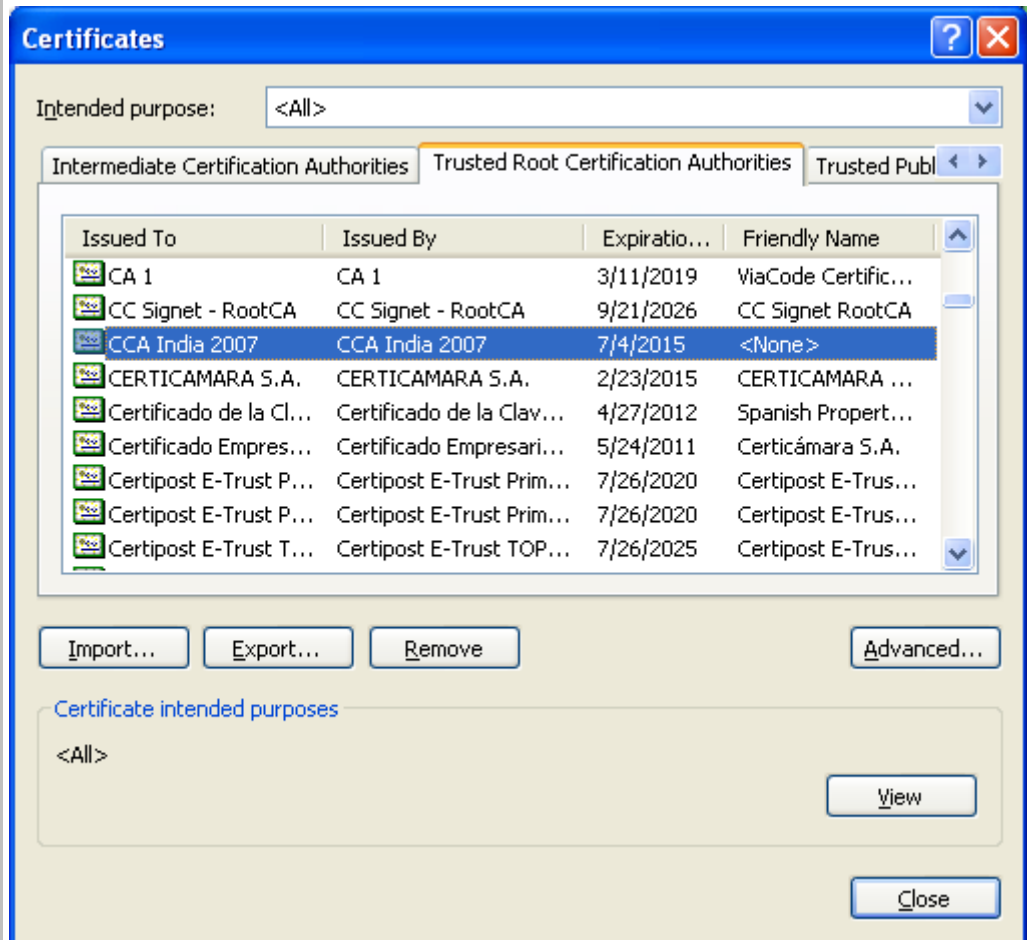


- x. To view the installed CCA certificate, open up a window of Microsoft Internet Explorer and then click on **Tools→Internet Options→Content**





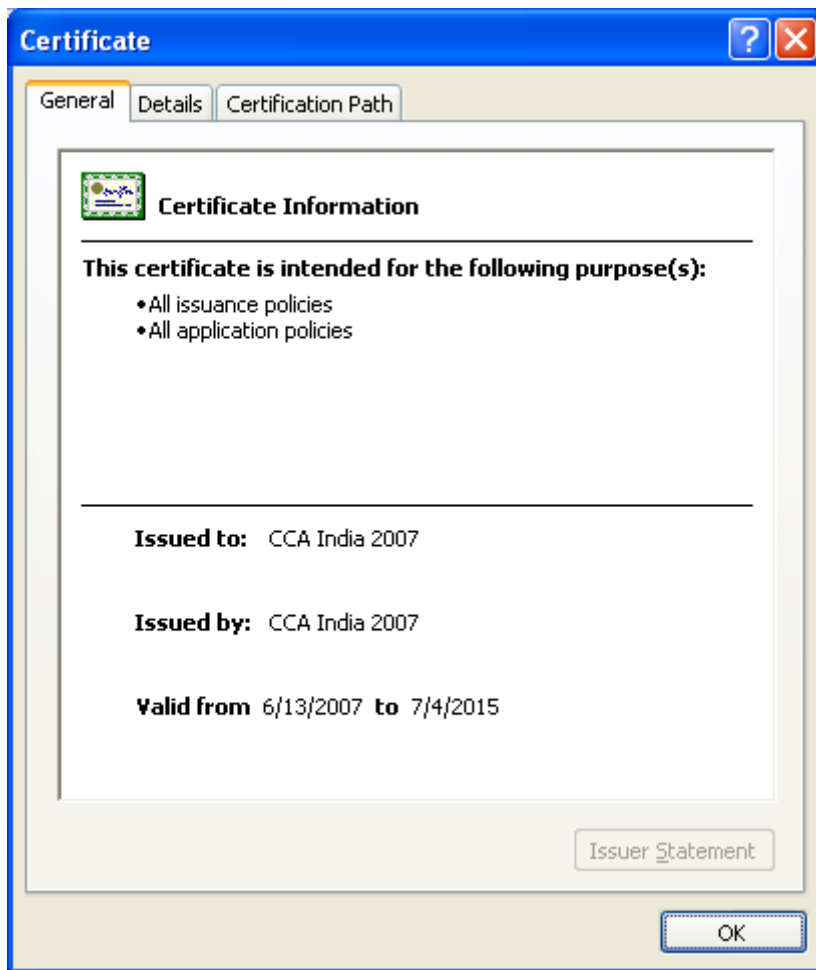
- xi. When the above window opens up, click on “**Certificates**” and then click on the “Trusted Root Certification Authorities” tab. The following screen will open up. Click on “**CCA India 2007**” and then click on “**View**”.



- xii. The certificate illustrated in the next page will now open up on your screen. Notice that when we had first seen this certificate while downloading it from the [www.cca.gov.in](http://www.cca.gov.in) website, it displayed the following notice:

“This CA Root certificate is not trusted.  
To enable trust, install this certificate in  
the Trusted Root Certification  
Authorities store”.

Now it does not display that notice. This is because we have installed it in the “Trusted Root Certification Authorities store” of our computer and thereby we have indicated to our computer that we trust this certificate.



## 2. Selecting a Certifying Authority

Visit the website of the Controller of Certifying Authorities at [www.cca.gov.in](http://www.cca.gov.in) to obtain a list of licenced Certifying Authorities in India. This website also provides the disclosure records of the various licenced Certifying Authorities. The links to the websites of these Certifying Authorities are also provided.

Based on this information and the study of the relevant websites, you can select a Certifying Authority. For this illustration we have selected the Tata Consultancy Services Certifying Authority (CA) which has the official website [www.tcs-ca.tcs.co.in](http://www.tcs-ca.tcs.co.in)

## 3. Visit the website of the Certifying Authority

A visit to the [www.tcs-ca.tcs.co.in](http://www.tcs-ca.tcs.co.in) website shows that the CA provides three types of digital signature certificates. The following information is provided in respect of these certificates:

### **Class-1 Certificates**

Class-1 Certificates are personal email Certificates that allow you to secure your email messages. These Certificates can be used to:



Digitally sign email - You can digitally sign your email messages using TCS-CA Personal Digital Certificate so that the recipient is assured that the email has come from you.

Encrypt email - You can encrypt emails using TCS-CA Personal Digital Certificate to prevent unauthorized people from reading it.

Authenticate to Web Servers - You can authenticate yourself to a Web Server to engage in secure communication with Web Server using TCS-CA Personal Digital Certificate. This protects all information such as credit card details that you send to the Web Server.

Class-1 Certificates however, do not facilitate strong authentication of the identity of the Subscriber; hence are not intended for, and shall not be relied upon, for commercial use where proof of identity is required.

### **Class-2 Certificates**

Class-2 Certificates are issued as Managed Digital Certificates to employees/ partners/ affiliates/ customers of business and government organizations that are ready to assume the responsibility of verifying the accuracy of the information submitted by their employees/ partners/ affiliates/ customers.

Class-2 Certificates are issued following a top down approach. The entire organization is treated as a Sub-CA/RA. The organization is given a Digital Certificate signed by TCS-CA to initiate the process of issuing Certificates to its employees/ partners/ affiliates/ customers. The Sub-CA/RA in turn requests the issue of Digital Certificates for employees/ partners/ affiliates/ customers of the organization from TCS-CA. In the case of a Class-2 Certificate, the verification of details supplied with the request for a Digital Certificate is done by the organization appointed as a Sub-CA/RA under the TCS-CA Trust Network.

Class-2 Certificates issued under the TCS-CA Trust Network are legally valid under the Indian IT Act 2000.

### **Class-3 Certificates**

Class-3 Certificates are issued to individuals, companies and government organizations. They can be used both for personal and commercial purposes. They are typically used for electronic commerce applications such as electronic banking, electronic data interchange (EDI), and membership-based on-line services, where security is a major concern.

The level of trust created by the Digital Certificate is based on the authentication procedures used by the CA to verify your identity and the service guarantees offered by the CA to back up that authentication.

TCS-CA uses various procedures to obtain evidence of your identity before issuing you the Class-3 Certificate. During verification, you will also need to be physically present before a Registration Authority (RA), qualified by TCS-CA due to their neutrality and reliability. These validation procedures provide stronger assurances of an applicant's identity.

Class-3 Certificates issued by the TCS-CA are legally valid under the Indian IT Act 2000.



#### 4. Select the type of certificate needed

We need a legally valid digital signature certificate for an individual. The relevant certificate is a **Class 3 certificate**.

#### 5. Submit an online request

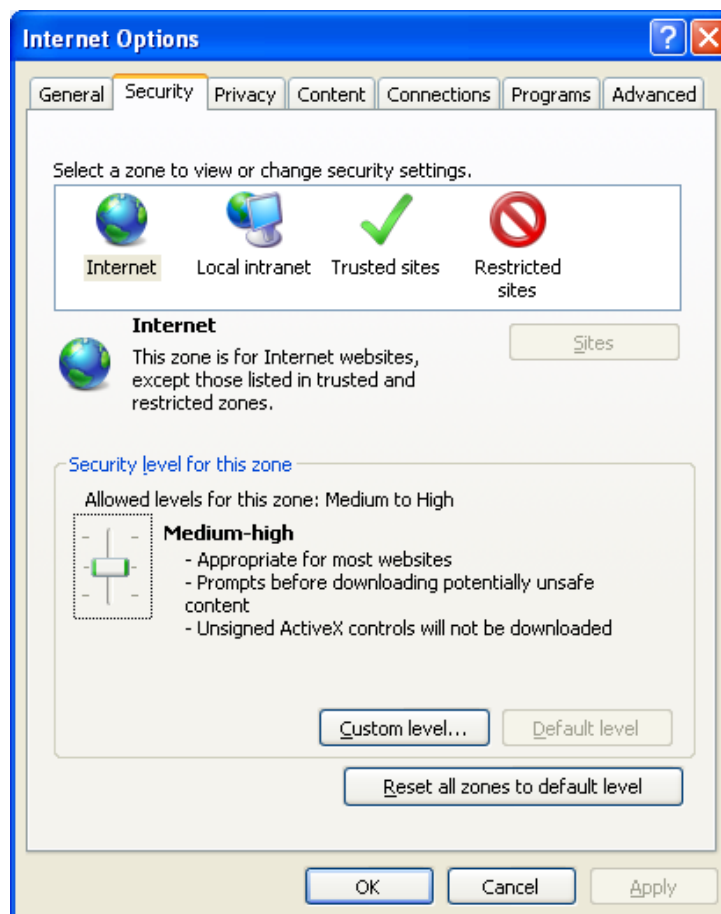
The next steps are to create a user account on the TCS CA website, complete an online enrollment form and generate a cryptographic key pair on our computer. The following issues have to borne in mind:

##### i. **Computer Requirements**

A computer running Microsoft Windows NT, 2000 or XP operating system is needed. Additionally, the computer must have Internet Explorer 5.5 or higher.

##### ii. **Browser Settings**

Active-X controls need to be enabled in the Internet browser. To do this go to Tools >> Internet Options >> Security and click 'Default Settings' and set to 'Medium'.





### iii. Enrollment Instructions

Cryptographic keys are generated and stored on our computer when we enroll for a digital certificate. Ownership of these keys forms the basis of our digital identity for digital signatures and encryption applications.

During enrollment we specify that we are enrolling for a **Signing Certificate (single key pair)**.

We also select “**Microsoft Enhanced Cryptographic Provider v1.0**” as the “Cryptographic Service Provider”.

| Contents of your Digital Certificate |  | Help ?                    |
|--------------------------------------|--|---------------------------|
| Common Name *                        | <input type="text" value="Rohas Nagpal"/>        | (eg: Anish K. Srivastava) |
| E-Mail Address *                     | <input type="text" value="rn@asianlaws.org"/>    | (eg: Anish@atc.tcs.co.in) |
| Organisation                         | Tata Consultancy Services - Certifying Authority |                           |
| Organisation Unit                    | TCS-CA - Registration Authority                  |                           |
| Organisation Unit                    | Individual - Others                              |                           |
| Address/Locality *                   | <input type="text" value="Pune"/>                | (eg: Mumbai)              |
| State *                              | <input type="text" value="Maharashtra"/>         | (eg: Maharashtra)         |
| Country Code                         | <input type="text" value="India"/>               | ▼                         |

**Select the Cryptographic Service Provider**

The Cryptographic Service Provider or CSP is a program that generates your public/private key pair.

NOTE : Indian IT Act stipulates that you use 1024 bit length keys. In case your browser does not support 1024 bit keys, your browser has to be updated with the relevant patches.

Choose the appropriate CSP below depending on where you plan to store your private key.

- If you are using the IE Browser, please select "Microsoft Enhanced Cryptographic Provider v1.0"
- For Aladdin eToken PRO select "eToken Base Cryptographic Provider"
- For Safenet iKey 1000 8k please select "Rainbow iKey 1000 RSA Cryptographic Service Provider"
- For Safenet iKey 2032 32k please select "Datakey RSA CSP"

Cryptographic Service Provider \*  ▼

**Subscriber Agreement**

By applying for, submitting, or using a Digital Certificate you are agreeing to the terms of the [TCS-CA Subscriber Agreement](#)

After filling in the details, we click on “**Generate Request**”.

We then confirm our details at the next screen and click on “**OK**”. We are then asked whether we want to request a digital signature certificate. Click on “**Yes**”.

The following screen will open up. Click on "OK".



The next screen will display the request number. Take a printout of this page and then click on "Go to Step 2".

The next screen informs us that paper copies of the following need to be submitted to TCS CA:

1. filled Certificate Request Form and
2. supporting Validation documents.

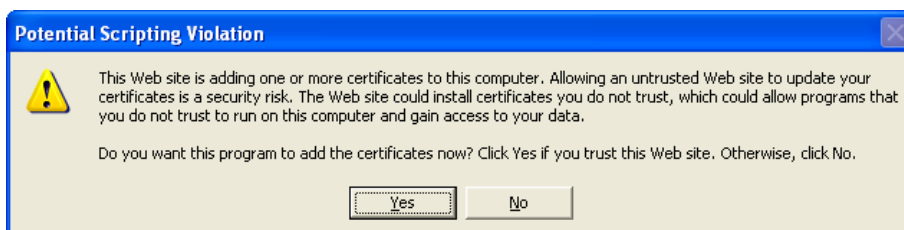
The Certificate Request Form can be downloaded from this page in Word Format as well as PDF Format.

An email is also received from TCS CA regarding the application made by us.

Until the certificate is generated and downloaded by us successfully, we must:

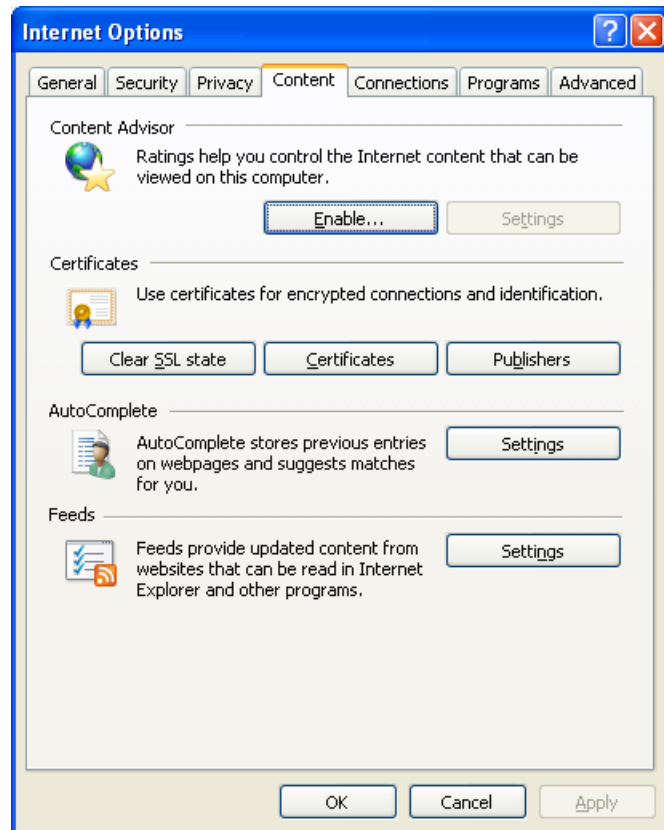
1. not format the computer
2. not re-install or upgrade the Internet Explorer

A few days later we receive an email from TCS CA informing us that the digital signature certificate is ready for download. Using the Authentication PIN provided in the email, the digital signature certificate can be downloaded after logging into the TCS CA website. While downloading the certificate, the following screen may pop up. Click on "Yes".

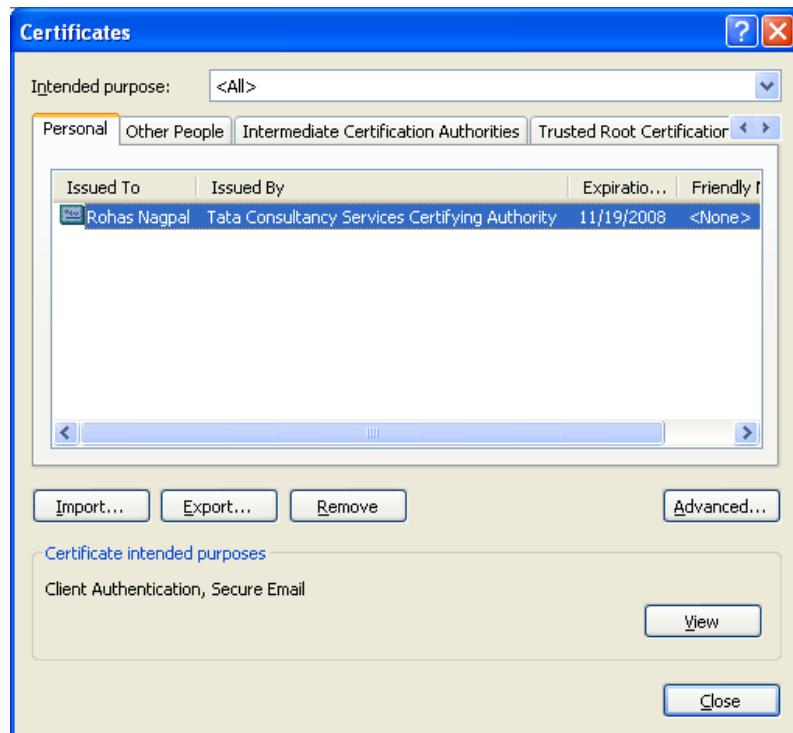




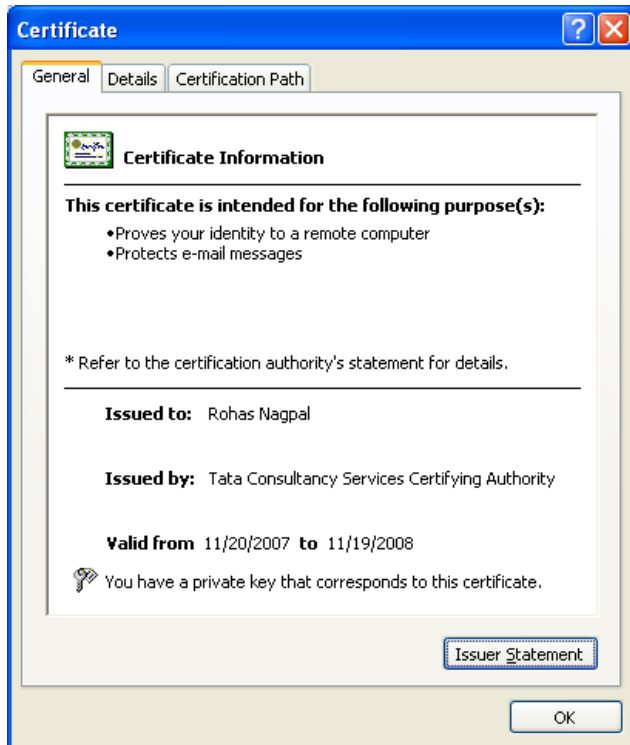
To view your digital signature certificate, open up a window of Microsoft Internet Explorer and then click on **Tools**→**Internet Options**→**Content**



Now click on “**Certificates**”.



Click on “**View**”.

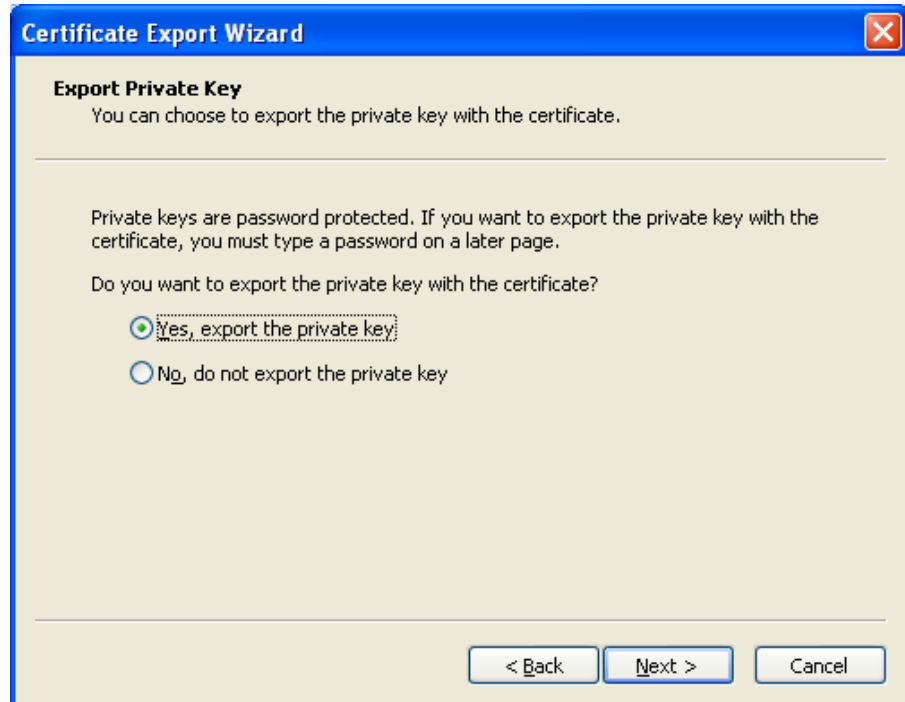


It is advisable to backup a copy of your digital signature certificate along with the private key to a secure location.

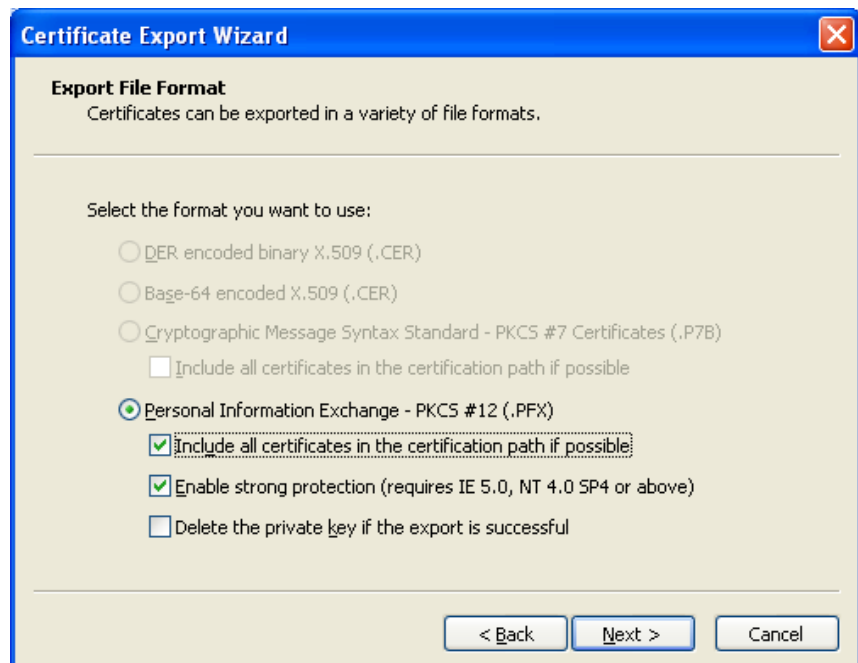
To do this, click on “**Export**” in the screen before this.



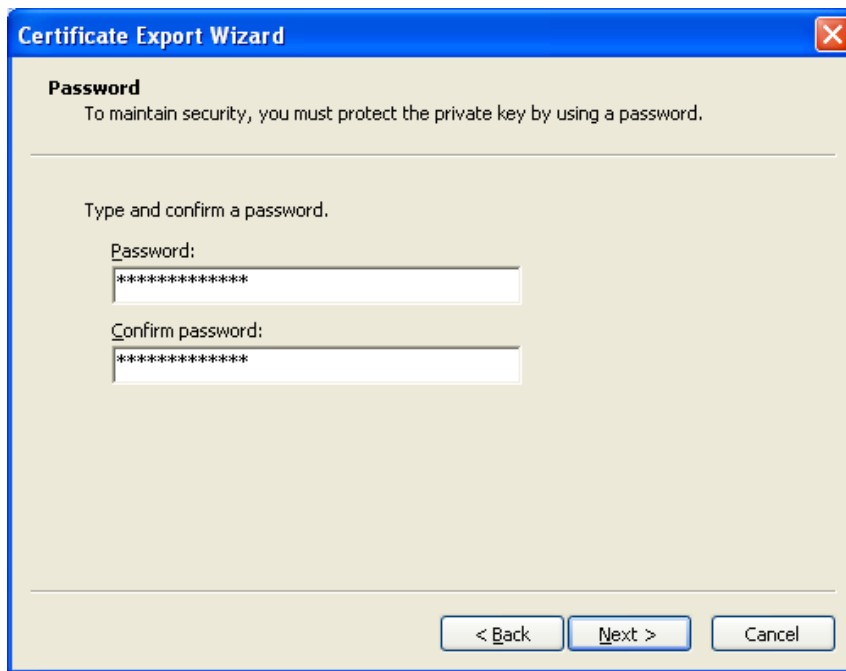
Click on “**Next**”.



Select the “**Yes, export the private key**” option and then click on “**Next**”.



Select the options marked above and click on “**Next**”.



**Certificate Export Wizard**

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

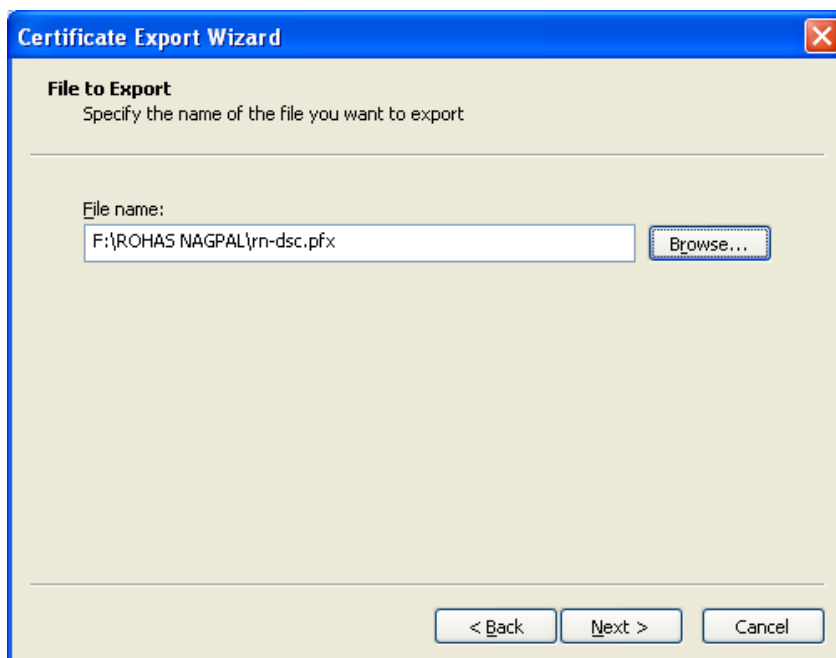
Type and confirm a password.

Password:  
\*\*\*\*\*

Confirm password:  
\*\*\*\*\*

< Back   Next >   Cancel

You will now need to enter a password. Ensure that you enter a complex password that is not known to anyone else. Then click on **“Next”**.



**Certificate Export Wizard**

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

File name:  
F:\ROHAS NAGPAL\rn-dsc.pfx   Browse...

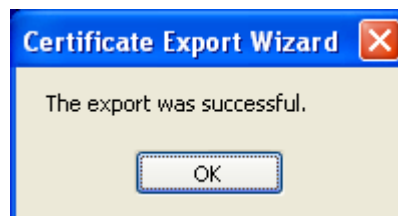
< Back   Next >   Cancel

After selecting a suitable location to save the digital signature certificate, click on **“Next”**.





Click on “**OK**” to complete the backup process. The following screen will then open up.







[www.asianlaws.org](http://www.asianlaws.org)

**Head Office**

6th Floor, Pride Senate,  
Behind Indiabulls Mega Store,  
Senapati Bapat Road,  
Pune - 411016.  
India

**Contact Numbers**

+91-20-25667148  
+91-20-40033365  
+91-20-64000000  
+91-20-64006464

**Email:** [info@asianlaws.org](mailto:info@asianlaws.org)

**URL:** [www.asianlaws.org](http://www.asianlaws.org)