**Rohas Nagpal** is the founder President of Asian School of Cyber Laws.

He advises Governments and corporates around the world in cyber crime investigation and cyber law related issues. He has assisted the Government of India in drafting rules and regulations under the Information Technology Act, 2000.

He has authored several books, papers and articles on cyber law, cyber terrorism, cyber crime investigation and financial law.

Rohas lives in Pune (India) and blogs @ rohasnagpal.com

---

**Some of the papers authored by Rohas Nagpal**

1. Internet Time Theft & the Indian Law
2. Legislative Approach to Digital Signatures
3. Indian Legal position on Cyber Terrorism
4. Defining Cyber Terrorism
5. The mathematics of terror
6. Cyber Terrorism in the context of Globalisation
7. Biometric based Digital Signature Scheme

---

**Some of the books authored by Rohas Nagpal**

![Book Covers](image_url)
DIGITAL SIGNATURES ................................................................. 2

1. OBTAINING A DIGITAL SIGNATURE CERTIFICATE .................. 4

2. DIGITALLY SIGNING EMAILS ...................................................... 19
Digital Signatures

Let us take an overview of this concept using a simple illustration.

Illustration
Sanya uses her computer to generate a public and private key pair. Simply put, these keys are very large numbers.

She then stores her private key very securely on her computer. She uploads her public key to the website of a licensed certifying authority (CA). She also couriers a filled in application form and photocopies of her passport and Income Tax PAN card to the CA.

After following some verification procedures, the CA sends Sanya a hardware device by post. This device contains Sanya’s digital signature certificate. The digital signature certificate contains Sanya’s public key along with some information about her and the CA.

Sanya then has to accept her digital signature certificate.

All digital signature certificates are stored in the online repository maintained by the Controller of Certifying Authorities.

Each Certifying Authority stores digital signature certificates issued by it in an online repository.

In order to digitally sign an electronic record, Sanya uses her private key.

In order to verify the digital signature, any person can use Sanya’s public key (which is contained in her digital signature certificate).

In case Sanya had originally generated her private key on a smart card or USB Crypto Token then the subsequent signatures created by her would be secure digital signatures.
Note: The smart card / crypto token have a chip built into it, which has crypto modules to enable the signing operation to happen in the device itself. The private key does not come out of the device in its original form.

In cases Sanya had generated and stored her private key on a hard disk, floppy, CD, pen drive etc then subsequent signatures are not secure digital signatures.
1. 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) 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 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.

   ![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:

![Certificate information window](image)

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:

![Certificate Import Wizard](image)
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”.

![Certificates](image)

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 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 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 is 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

3. **Visit the website of the Certifying Authority**

A visit to the 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”.

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".
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”.

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.

The export was successful.

OK
2. Digitally signing emails

This chapter serves as a step by step guide for digitally signing emails using Microsoft Outlook (version 2003 is used in this chapter). The basic steps are as under:

1. Configure your email account using Microsoft Outlook. The exact information to be entered (such as server details etc) would depend upon the email service used by you. The image below illustrates the basic configuration for a gmail account.

![Email Configuration Screenshot](image-url)
2. Go to the **Tools → Options → Security** option of Microsoft Outlook.

The following screen opens up.

![Options Screen](image)

Check the "**Add Digital Signatures to outgoing messages**" option. Then click on "**Settings**". The following screen will open up.

![Change Security Settings Screen](image)
Click on the “Choose” button next to the Signing Certificate option. The following screen will open up.

**Note:** In this illustration we are going to use the digital signature certificate issued to Rohas Nagpal having the email ID rn@asianlaws.org

Click on “OK”. The following screen will open up.

Add a suitable title for the Security Settings Name (e.g. “Rahas Nagpal” in this case). Then click on “OK”.

© 2008 Rohas Nagpal. All rights reserved.
The following screen will open up.

![Options](image)

Click on “**Apply**” and then click on “**OK**”.

Now compose and send an email. All emails sent using the `rn@asianlaws.org` account will be automatically signed. Let us presume that an email has been sent from `rn@asianlaws.org` to `sanyanagpal@gmail.com`

The `sanyanagpal@gmail.com` account is accessed by Sanya Nagpal using Microsoft Outlook. When Sanya received the digitally signed email from Rohas Nagpal, it will appear as under:

![Hello - Message (HTML)](image)
Notice the icon marked with a circle in the image above. Clicking on it opens up the following screen:

**Digital Signature: Valid**

Subject: Hello  
From: Rohas Nagpal  
Signed By: rm@asianlaws.org

The digital signature on this message is Valid and Trusted.

For more information about the certificate used to digitally sign the message, click Details.

[Details…]

Warn me about errors in digitally signed e-mail before message opens.

[Close]

It is clearly stated that “The digital signature on this message is Valid and Trusted”. Clicking on the “Details” button opens up the following screen:

**Message Security Properties**

Subject: Hello

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

**Security Layers**

Select a layer below to view its description.

- Subject: Hello
- Digital Signature Layer
- Signed by rm@asianlaws.org

Description:

OK: Signed by rm@asianlaws.org using RSA/SHA1 at 5:34:04 PM 11/22/2007.

Click any of the following buttons to view more information about or make changes to the selected layer:

[Edit Trust…]  [View Details…]  [Trust Certificate Authority…]

Warn me about errors in digitally signed e-mail.

[Close]
Clicking on “View Details” shows the relevant signature information as under:

**Signature Information**
- **Message format:** 5/MIME
- **Signed by:** rmb@asianlaws.org
- **Signature status:** OK
- **Signing time:** 5:54:04 PM 11/20/2007
- **Digest algorithm:** SHA1
- **Signature algorithm:** RSA (1024-bits)

**Certificate Information**
- **Issued by:** Tata Consultancy Services Certifying
- **Certificate status:** OK
7. Digitally signing Word documents

This chapter serves as a step by step guide for digitally signing Microsoft Word documents (version 2003 is used in this chapter). The basic steps are as under:

1. **Create** the Microsoft Word document that you want to digitally sign.
2. **Save** the document to a suitable location.
3. **Open** the document and then **click on Tools → Options → Security**
4. The following screen will open up. Click on “Digital Signatures”.

5. The following screen will open up.
6. Click on "Add". The following screen will open up:

7. Click on "OK". The following screen will open up.
3. Click on “OK”. In the next screen that opens up click on “OK” again. The document is now digitally signed.

4. Whenever the document is opened, the following message will be displayed at the bottom of the screen:

   A5C1.doc: 1,468 characters. (This document contains digital signatures)

5. Once the document opens up, the following icon will be displayed at the bottom of the screen.

6. On double clicking the icon the following screen opens up and displays information about the signer of the document.
Head Office

6th Floor, Pride Senate,
Opp International Convention Center,
Senapati Bapat Road,
Pune - 411016.
India

Contact Numbers
+91-20-25667148
+91-20-40033365
+91-20-65206029
+91-20-6400 0000
+91-20-6400 6464
Fax: +91-20-25884192

Email: info@asianlaws.org
URL: www.asianlaws.org