# **Digitally signing emails**

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

# 6. 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:

 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.

E-mail Accounts			
Internet E-mail Each of these	Settings (POP3) e settings are required to g	get your e-mail account working.	×.
User Informatio	n	Server Information	
Your Name:	anya Nagpal	Incoming mail server (POP3):	pop.gmail.com
<u>E</u> -mail Address: s	anyanagpal@gmail.com	Outgoing mail server (SMTP):	smtp.gmail.com
Logon Informati	on	Test Settings	
User Name: s	anyanagpal@gmail.com	After filling out the information	on this screen, we
Password:		button below. (Requires netwo	ound by clicking the ork connection)
	<u>R</u> emember password	Test Account Settings	
Log on using Se	cure Password (SPA)		
Hactorication	.5. 67		More Settings
		< <u>B</u> ack	Next > Cancel
E-mail Settings		Internet E-ma	ail Settings
Outgoing Server Connection	Advanced	General Outg	going Server Connection Advanced
outgoing server (SMTP) requires a	authentication	Server Port N	Jumbers
lse same settings as my incoming Log on using	mail server	Incoming se	server (POP3): 995 Use Defaults server requires an encrypted connection (SSL)
User <u>N</u> ame:		Outgoing se	erver (SMTP): 465
Password:		V This	server requires an encrypted connection (SSL)
Log on using <u>S</u> ecure Password	Authentication (SPA)	Server <u>T</u> imeo	uts Long 1 minute
.og on to incoming mail server bef	ore sending mail	Delivery —	Long Thindo
		Leave a	copy of messages on the server
		Rem	iove from server after 🛛 10 🔅 days
		Rem	ove from server when deleted from 'Deleted Item



2. Go to the **Tools**  $\rightarrow$  **Options**  $\rightarrow$  **Security** option of Microsoft Outlook.

The following screen opens up.



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

Change Security Settin	gs	×
Security Setting Preferences Security Settings Name:		
		*
Cryptography <u>F</u> ormat:	S/MIME	~
Defaul <u>t</u> Security Sett	ing for this cryptographic message format	
Default Security	Setting for all cryptographic <u>m</u> essages	
Security Labels	New Delete Password	
Certificates and Algorithms		
Signing Certificate:	hoose.	
Hash <u>A</u> lgorithm:	×	
Encryption Certificate:	Choose.	
Encryption Algorithm:	×	
Send these certificat	es with signed messages	
	OK Cancel	



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

Select Certific	ate			? 🛛
Select the certifi	ate you want to	use.		
Issued to	Issued by	Intended P	Friendly na	Expiration
📟 Rohas N	Tata Consu	Client Auth	None	11/19/2008
<				>
		ж Са	ncel <u>V</u> iev	v Certificate

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

Change Security Setti	ngs	$\mathbf{X}$
Security Setting Preference	·s	_
<u>S</u> ecurity Settings Name	:	
		~
Cryptography <u>F</u> ormat:	S/MIME	~
Defaul <u>t</u> Security Sel	ting for this cryptographic message format	
Default Securit	y Setting for all cryptographic messages	
Security Labels	. <u>N</u> ew <u>D</u> elete <u>Password</u>	
Certificates and Algorithms		_
Signing Certificate:	Rohas Nagpal	
Hash <u>A</u> lgorithm:	SHA1	
Encryption Certificate:	Rohas Nagpal	
Encryption Algorithm:	3DES 🗸	
Send these certifica	tes with signed messages	
	OK Cancel	

Add a suitable title for the **Security Settings Name** (e.g. "Rohas Nagpal" in this case). Then click on "**OK**".



#### The following screen will open up.

Options	? 🗙
Preference	ces Mail Setup Mail Format Spelling Security Other
Encrypt	ed e-mail
2	Encrypt contents and attachments for outgoing messages   Add digital signature to outgoing messages Image: Content of the second sec
	Send clear <u>t</u> ext signed message when sending signed messages
	<u>Request S/MIME receipt for all S/MIME signed messages</u>
	Default Setting: Rohas Nagpal 🛛 Settings
Security	Zones
0	Security zones allow you to customize whether scripts and active content can be run in HTML messages.
	Zone: 🚫 Restricted sites 🛛 Zone Settings
Downloa	ad Pictures
	Change Automatic Download Settings
Digital II	Ds (Certificates)
UT OF OF	Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.
	Import/Export
	OK Cancel Apply

Click on "Apply" and then click on "OK".

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

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

🖂 He	llo - M	essage	(HTML	)							
Eile E	<u>E</u> dit	⊻iew	Insert	F <u>o</u> rmat	<u>P</u> GP	<u>T</u> ools	<u>A</u> ctions	<u>H</u> elp	Adobe	PDF	
: 🕰 R	eply   🦻	💫 Reply	y to All	🙈 For <u>w</u> a	rd   🛃		*   8	🔌   [	🖰 🗙	<b>4</b> •	++ 7
From To: Cc: Subje Signe	i: Sa sa ect: He ed By:	Roha anyanag ello rn@a	s Nagpal    pal@gma  sianlaws.	[rn@asian il.com org	laws.org	1] Se	nt: Tue	11/20/20	007 5:34	РМ	
Hi, This	s is a t	est me	essage.								
Reg Roh	ards, as Nag	gpal	5								
											$\sim$

Notice the icon marked with a circle in the image above. Clicking on it opens up the following screen:



Digital S	ignature: Valid 🛛 🔀
Subject: From:	Hello Rohas Nagpal
Signed By	: rn@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.
Warn i	me about errors in digitally signed e-mail before message opens.
	Gose

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. <b>Security Layers</b>
Select a layer below to view its description.
✓ Subject: Hello
Signer: m@asianlaws.org
Description:
OK: Signed by rn@asianlaws.org using RSA/SHA1 at 5:34:04 PM
11/20/2007.
Click any of the following buttons to view more information about or make
changes to the selected layer:
Edit Trust
<u>W</u> arn me about errors in digitally signed e-mail. <u>⊆</u> lose



Clicking on "View Details" shows the relevant signature information as under:

Signature	? 🛛						
General Details							
Signature In	formation						
Message format:	Message format: 5/MIME						
Signed by:	rn@asianlaws.org						
Signature status:	ок						
Signing time:	5:34:04 PM 11/20/2007						
Digest algorithm:	SHA1						
Signature algorithm	n: RSA (1024-bits)						
Certificate Ir	nformation						
Issued by:	Tata Consultancy Services Certifying 📃						
Certificate status:	ок						
	<u>V</u> iew Certificate						



## **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 URL: www.asianlaws.org