Importing and Using your Email or Personal Authentication certificate with Mozilla SeaMonkey Email Client (PC)

- If you originally applied for the certificate on the same computer as your SeaMonkey installation then it should already be installed. You can skip straight to 'Signing and Encrypting'.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides using one of the browsers listed on the CPAC main page. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then follow the 'import' instructions in this document.

Importing your certificate into Mozilla SeaMonkey

Signing and Encrypting mails

Importing your Certificate into Mozilla SeaMonkey:

- 1. Open SeaMonkey and then click 'Edit' > 'Preferences'.
- In the Preferences screen, select 'Privacy & Security' > 'Certificate' and then click the 'Manage Certificates...' button.
- 3. In the certificate manager interface, make sure the 'Your Certificates' tab is selected and click 'Import'.



10	green@co		y.com -	SeaMon	ikey
	<u>dit V</u> iew	<u>G</u> o	<u>M</u> essage	e <u>T</u> ools	Window
Ľ	<u>U</u> ndo Redo			Ctrl+Z	
t Ms	<u>10</u> 000			Curri	rwar
ew:	Cu <u>t</u> Copu			Ctrl+X	
ne	Paste			Ctrl+V	
Lc	<u>D</u> elete Fo	ilder		Del	on
	Select				
<u> </u>					nts
1 21	Eind in Th Find Adai	iis Mess n	;age	Ctrl+F Ctrl+G	<u>WK Si</u>
	Find Prev	ious		Ctrl+Shif	ft+G eate
-	Find Links	As You	i Type	1	
	Find Te <u>x</u> t	As You	л Туре	1	
-	Propertie	5			
	Mail & Ne	wsgrou	ips Accour	nt Settings	S
\bigcirc	Pr <u>e</u> ferenc	es			
	🥩 P	refer	ences		
		ategory Not	/ tifications	~	Certificates
		Cor	mposition		
		Ser	1d Format		Client Certificate Selection Decide how SeaMonkey selects a security certificate to precent to websites
		Add	dressing		that require one:
		Jun	ik & Suspe	et	Select Automatically Ask Every Time
		Tag	ļs		
		Ret	urn Recei:	pts	Manage Certificates
		Cha	aracter En	.cod	Use the Certificate Manager to manage your personal certificates, as well
		Net	work & St	ora	as these of other people and certificate authorities.
		Compo	ser		Manage Certificates
		Chat7il	a		
		Privacy	/ & Securit	y >	Manage Sectinity Devices
		Priv	/ate Data		Use this button to manage your security devices, such as smart cards.
		Cod	okies		Manage Security Devices
		Ima	ages		
		Рор	oup Windo	ws	
		Pas	swords		
		Mas	ster Passv	vords	
		SSL	-		
		Cer	tificates		
		vair	uacion	~	
					OK Cancel Help
_					V
4	Certific	ate M	anager		
	Your Certif			Servers A	Authorities Others
		icates	People :	JOI YOI J P.	
	Va F.	icates	People		
	You have	ficates e certif	People	m these or	rganizations that identify you:
	You have	ficates e certif tate Na	People icates from me	m these or Securit	irganizations that identify you: ity Device Serial Number Expires On 🛱
	You have	^f icates e certif :ate Na	People icates fro	m these or Securit	rganizations that identify you: ity Device Serial Number Expires On 四
	You hav	ficates e certif ate Na	People icates fro	m these or	irganizations that identify you: ity Device Serial Number Expires On 🖽
	You hav Certific	icates e certif	People icates from	m these or	organizations that identify you: ity Device Serial Number Expires On 🖪
	You hav Certific	icates e certif	People ficates from me Backu	m these or	arganizations that identify you: ity Device Serial Number Expires On E Backup All Import Delete
	You hav Certific	Ficates e certif tate Na	People icates fro me Backu	m these or Securit	action All

- 4. Navigate to the location of the PKCS12 certificate file in which your certificate is stored and enter any necessary passwords. Your certificate will be imported and you will be able to use it to digitally sign and encrypt e-mails.
- 5. Click OK in the Certificate Manager dialog to return to the Preferences screen.
- 6. Optional select Ask me every time under When a server requests my personal certificate.

Doing this alerts you to the fact that a server has requested identity confirmation and enables you to select your Comodo Personal Authentication Certificate.

7. Click OK in the Preferences interface to return to SeaMonkey.

That's it. You have successfully imported your Comodo Personal Authentication certificate into Mozilla SeaMonkey.

Signing and Encrypting Mails

- Signing an email ensures the recipient knows the email has come from you and informs them that it has not been modified in transit.
- Encrypting an email ensures that only the recipient can read the email content and attachments.

Note: In order to encrypt mail, you must first have your recipient's email certificate in your certificate store. To obtain their certificate, you need to get your contact to send you a signed email. Upon receipt of the signed mail, their certificate will be automatically imported into your certificate store and you will be able to sign/encrypt mail to that person.

Assign the certificate Signing and encrypting individual mails

Signing and encrypting all mails by default

Assign the certificate

- 1. Open SeaMonkey and select 'Edit' then 'Mail & Newsgroups Account Settings...'.
- 2. In the 'Mail & Newsgroups Account Settings' screen, select 'Security'.

COMODO Creating Trust Online[™]

Mail & Newsgroups Account Se	ettings						
alicegreen@company.com	Security						
Copies & Folders Composition & Addressing	To send and receive signed or encrypted messages, you should specify both a digital signing certificate and an encryption certificate.						
Synchronization & Storage Return Receipts	Use this certificate to digitally sign messages you send:						
Security Encodel Folders	Digitally sign messages (by default)						
Junk Settings Disk Space	Encryption Use this certificate to encrypt & decrypt messages sent to you:						
Outgoing Server (SMTP)	Select Clear Default encryption setting when sending messages: • • Never (do not use encryption) • Required (can't send message unless all recipients have certificates)						
	Certificates Manage Certificates Manage Security Devices						
Add Account							
Set as De <u>f</u> ault							
Remove Account							
	OK Cancel <u>H</u> elp						

- 3. Click **'Select'** beside the text box in the **'Digital Signing'** area and select your Comodo Personal Authentication certificate from the list.
- 4. Click 'OK'.
- 5. Select the same certificate for Encryption by clicking Yes in the confirmation dialog.

SeaMonkey							
?	You should also specify a certificate for other people to use when they send you encrypted messages. Do you want to use the same certificate to encrypt & decrypt messages sent to you?						
	<u>Y</u> es <u>N</u> o						

6. Click OK in the Mail & Newsgroups Account Settings interface to finalize your settings.

Signing and encrypting individual mails

To sign an individual mail:

1. Compose your email and attach files as usual.



2. Click Security and choose Digitally Sign This Message.

-	Compose: Market Analysis Document									
1.11	<u>F</u> ile	<u>E</u> dit <u>V</u> iev	v <u>I</u> nsert	F <u>o</u> rmat	Option	s <u>T</u> ools	<u>W</u> indow	Help		
•	Send	Addres	Attach	- 🚳	•	🙆 - Security	Save	•		9
•	From: Alice G <alicegreen@company.com> Encrypt This Message</alicegreen@company.com>							Attachments:		
	To: Dohn Smith < johnsmith				hnsmit	Digitally Sign This <u>M</u> essage			Market Analysis D13.odt (1	0.3 KB)
						View Se	curity <u>I</u> nfo			
	Subject: Market Analysis Document									
(CAN)	Body 1	fext 🔽		/idth			A	B <i>T</i>		₹·[

A pen icon \swarrow will appear in the status bar, indicating that the message is digitally signed.

3. Click the Send button.

To encrypt each mail:

- 1. Compose your email and attach files as usual.
- 2. Ensure the recipient has a Digital Certificate and you have assigned the Certificate to their entry in your contacts area.
- 3. Click Security and choose Encrypt This Message.

-	🛠 Compose: Sales Report 📃 🗖 🔯								
•	Eile	<u>E</u> dit <u>V</u> iew	Insert	F <u>o</u> rmat (Options	<u>T</u> ools	<u>W</u> indow	<u>H</u> elp	
•	Send	Address	2 Attach	- Spell	- Sec	🔂 🔸	Save	·	9
	From:	Alice G <a< th=""><th>icegreen@</th><th>company.cor</th><th>n></th><th colspan="3">Encrypt This Message</th><th>Attachments:</th></a<>	icegreen@	company.cor	n>	Encrypt This Message			Attachments:
	To: A John Smith < johnsmit			nsmit 🖌	✓ Digitally Sign This Message View Security Info			Sales_Report_Sep13.odt (10.3 KB)	

A key icon ? will be displayed in the status bar indicating that the message and the attachments are encrypted.

4. Click the **Send** button.

Signing and Encrypting all mails by default:

- 1. Open SeaMonkey and then click 'Edit' > 'Mail & Newsgroups Account Settings'.
- 2. In the 'Mail & Newsgroups Account Settings' screen, select 'Security'.

Mail & Newsgroups Account Set	ttings 🛛 🔀
 alicegreen@company.com Server Settings Copies & Folders Composition & Addressing Junk Settings Synchronization & Storage Peturn Receipts Security Local Folders Junk Settings Disk Space Outgoing Server (SMTP) 	Security To send and receive signed or encrypted messages, you should specify both a digital signing certificate and an encryption certificate. Digital Signing Use this certificate to digitally sign messages you send: 50d996c3b2b4003113207a8f41a4e546_859d5f2; Digitally sign messages (by default) Encryption Use this certificate to encrypt & decrypt messages sent to you: 50d996c3b2b4003113207a8f41a4e546_859d5f2; Select Clear Default encryption setting when sending messages: Never (do not use encryption) Required (can't send message unless all recipients have certificates) Certificates Manage Certificates
Add Account	
Set as De <u>f</u> ault	
Remove Account	
	OK Cancel <u>H</u> elp

- 3. Select the appropriate options in the 'Digital Signing' and 'Default Encryption Settings...' areas to sign and/or encrypt your mails by default.
- 4. As a rule of thumb, many users choose to digitally sign by default but only encrypt when sending a message which requires confidentiality.
- 5. Click 'OK'.

About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.	Comodo CA Limited
1255 Broad Street	3rd floor, Office Village Exchange Quay
Clifton, New Jersey 07013	Trafford Road, Salford, Manchester M5 3EQ
United States	United Kingdom
Tel : +1.888.266.6361	Tel:+44 (0) 161 874 7070
Tel : +1.703.581.9361	Fax : +44 (0) 161 877 1767
Email: sales@Comodo.com	

For additional information on Comodo - visit https://www.comodo.com