YATANARPON TELEPORT COMPANY LTD.,

Yatanarpon Certification Authority

USER MANUAL FOR SECURE E-MAIL WINDOW LIVE MAIL (VISTA)

Yatanarpon Teleport Company Ltd., Hlaing Universities Campus, Hlaing Township, Yangon, Myanmar Ph: 951-652233, Fax: 951-652244 Email:<u>opetraingca@myanmar.com.mm</u> URL: <u>http://www.yatanarponca.com.mm</u>

Table of Contents

- 1. Creating Email Account in Window live Mail
- <u>Certificate Installation</u>
 Subscriber/ User Certificate installation
 - 2.2 CA certificate Installation (.CER)
 - 2.3 Root certificate Installation (.cer) File
 - 2.4 How to get Digital ID
 - 2.4.1 Downloading and Importing a Digital ID
 - 2.5 Importing Digital ID to Contacts
- 3. Certificate Application
 - 3.1 Signing Individual E-Mail
 - 3.2 Signing All Outgoing E-Mail
 - 3.3 Individual Encrypting your E-mail
 - 3.3.1 Encrypting Individual Messages
 - 3.3.2 Encrypting All Outgoing E-Mail
- 4. Things to Know
 - 4.1 How to protect your digital IDs
 - 4.1 What to do if a digital ID is lost or stolen
 - 4.2 Sharing certificates with others

1. Creating E-mail Account in Window Live Mail

To create email account setting in Window Live Mail:

- 1. Go to **Menu** bar and select **Tools** and scroll down to **Account**.
- 2. Click Add button

ernet Accounts		2
et up new e-mail accounts or newsgroup subscriptions by c fo make changes, export, or remove an account or subscript		
Mail	×	
203.81.71.104 (default) operatingca@myanmar.com.mm	Add	
News	<u>Remove</u>	
Microsoft Communities (default) msnews.microsoft.com	Properties	
Directory Service	Set as Defau	ılt
	Import	
	Export	
	Set Order	•
	Close	

- 3. You will see Select Account Type Dialog and choose Email Account.
- 4. Click **Next** button.

©	
Select Account Type What type of account would you like to add?	
What type of account would you like to add:	
	Next Cancel

- 5. Type your name in the following **Display name:** text box.
- 6. Then click **Next** button.

G		×
Your Name		
When you send e-mail, y Type your name as you v	our name will appear in the From field of the outgoing messa rould like it to appear.	ge.
<u>D</u> isplay name:	operatingca For example: John Smith]
Where can I find my e-m	il account information?	
		Net Coul
		<u>N</u> ext Cancel

- 7. Type your Email address in **E-Mail Address :** text box.
- 8. Click **Next** button.

Internet E-mail Address		
Your e-mail address is the	address other people use to send e-mail messages to you.	
<u>E</u> -mail address:	operatingca@myanmar.com.mm	
	For example: someone@microsoft.com	
Where can I find my e-ma	ail account information?	
		Next Cancel

 Type mail server numbers in Incoming e-mail server type:, Incoming mail (POP3 or IMAP) server and Outgoing E-Mail Server (SMTP) name. The following numbers are mail servers used for myanmar.com.mm.

Set up e-mail servers	
Incoming e-mail <u>s</u> erver type:	
Incoming mail (POP3 or IMAP) server:	
203.81.71.104	
Qutgoing e-mail server (SMTP) name: 203.81.71.114	
Outgoing server requires authentication Where can I find my e-mail server information?	
	Next Cancel

10. Then you will see Mail logon and fill up your password, then click Next.

Internet Mail Logon		
Type the account name	and password your Internet service provider ha	as given you.
E-mail usern <u>a</u> me:	operatingca	
Password:	•••••	
	☑ Remember pass <u>w</u> ord	
		Next Cance

Finally your account creation is finished. If you don't want to download your mail at this time, mark (**Do not download my email at this time**), and click **Finish** button.

Contraction of the second seco	×
Congratulations You have successfully entered all of the information required to set up your account. To save these settings and download your e-mail, click Finish. Do not download my e-mail at this time	
	<u>Finish</u> Cancel

2. <u>Certificate Installation.</u>

To use digital ID in your system, you need to install 3 certificate files as follow;

- 1. Subscriber/ User Certificate Installation (.PFX) File
- 2. Certification Authority (.CER) File
- 3. Root Certification Authority (.CER) File as provided by the CA.

2.1 <u>Subscriber/User Certificate installation</u>

- 1. Click your certificate (.pfx) file.
- 2. You will see Certificate Import Wizard, click Next button.
- 3. Specify the file you want to import by clicking **Browse** button and choose your file then click **Next** button.
- 4. To maintain security, the private key was protected by password. Type the password for the private key.

5. You can select all **Check** buttons or can choose one you like and click **Next** button.

Certificate Import Wizard	x
Password To maintain security, the private key was protected with a password.	
Type the password for the private key. <u>P</u> assword:	
•••••	
 Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option. Mark this key as exportable. This will allow you to back up or transport your keys at a later time. 	
Include <u>a</u> ll extended properties.	
Learn more about protecting private keys	
< <u>B</u> ack Next > Cance	3 3

6. Select **Place all Certificate in the following store** & click **Browse** button. You will see the **Select Certificate Store dialog** and choose the **Certificate Store**.

tificate I	mport Wizard
Certifica	te Store
Cer	ificate stores are system areas where certificates are kept.
	dows can automatically select a certificate store, or you can specify a location for certificate.
(Automatically select the certificate store based on the type of certificate
(Place all certificates in the following store
	Certificate store:
	Browse
Learn mo	re about <u>certificate stores</u>
	< <u>B</u> ack Next > Cancel

 Select the Personal folder and click OK button. Then click Next button in Certificate Store status window.

Select	the <u>c</u> ertificate store you want to use.
	Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates
E Sho	w physical stores

8. If you have successfully completed the **Certificate Import Wizard**, click **Finish** button.

Certificate Import Wizard	1000	
	Completing the Certificate Import Wizard The certificate will be imported after you click Finish.	
	You have specified the f	ollowing settings:
	Certificate Store Select Content File Name	ted by User Personal PFX C:\Users\K N Lwin\De
	٠ (m	F
	< <u>B</u> ac	k Finish Cancel

9. Click **OK** button to finish Certificate installation.

Certifica	ite Import Wizard 🛛 🔀
(į)	The import was successful.
	ОК

2.2 CA certificate Installation (.CER)

Second step is to install CA certificate (MET.cer) file.

- 1. Click the required (MET.cer) file.
- 2. Click Install Certificate button and follow the steps.

eneral	Details Certification Path
-	Certificate Information
Thi	s certificate is intended for the following purpose(s):
	Ensures the identity of a remote computer Proves your identity to a remote computer Ensures software came from software publisher Protects software from alteration after publication Protects e-mail messages Allows data to be signed with the current time
	Issued to: MET
	Issued by: myanmar infotech rootca
	Valid from 09/03/2009 to 09/03/2012
earn n	Install Certificate Issuer Statemen

3. Select **Place all Certificate in the following certificate store** and click **Browse** button to select the **certificate store**:..

Certificate Store	
Certificate stores are system are	as where certificates are kept.
Windows can automatically select the certificate.	t a certificate store, or you can specify a location for
Automatically select the ce	rtificate store based on the type of certificate
Place all certificates in the	following store
Certificate store:	
	Browse
earn more about <u>certificate stores</u>	
earn more about <u>certificate stores</u>	
earn more about <u>certificate stores</u>	

4. Select the **Intermediate Certification Authorities** folder and click **OK** button. Then click Next button in Certificate Store status window.

-	Personal
	Trusted Root Certification Authorities
	Enterprise Trust
	Intermediate Certification Authorities
	Trusted Publishers
	Untrusted Certificates

5. You will see again **Certificate Store status window** and follow the steps. Click **Finish** button to complete the **Certificate Import Wizard**.

Certificate Import Wizard	
	Completing the Certificate Import Wizard
	The certificate will be imported after you click Finish.
67	You have specified the following settings:
	Certificate Store Selected by User Intermediate Certifica Content Certificate
	4 [
	< Back Finish Cancel

6. When the Certificate Import Wizard is completed, click OK button.



2.3 Root certificate Installation (.cer) File

Third step is to install Root CA certificate (.cer) file.

- 1. Click (Myanmar Infotech Rootca .cer) file.
- 2. Click Install Certificate button and then click Next button.

Certificate
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s): All issuance policies All application policies
Issued to: myanmar infotech rootca
Issued by: myanmar infotech rootca
Valid from 09/03/2009 to 09/03/2014
Install Certificate Issuer Statement
ОК

- 3. Select **Place all Certificate in the following store** and click **Browse** button.
- 4. Select Trusted Root Certification Authorities folder in Select Certificate Store.

ertificate Store Certificate stores are system are	as where certificates are kept.
Windows can automatically select	a certificate store, or you can specify a location for
the certificate.	
Automatically select the ce	rtificate store based on the type of certificate
Place all certificates in the	following store
Certificate store:	
	Browse
arn more about <u>certificate stores</u>	
arn more about <u>certificate stores</u>	
am more about <u>certificate stores</u>	
arn more about <u>certificate stores</u>	< Back Next > Cance

····	Personal	
	Trusted Root Certification	Authorities
	Enterprise Trust	
	Intermediate Certification A	Authorities
	Trusted Publishers	
	Intrusted Certificates	
	III	

5. Click Finish button in **Certificate Import Wizard** dialog.

Certificate Import Wizard	Completing the Certificate Import Wizard
	The certificate will be imported after you click Finish. You have specified the following settings:
	Certificate Store Selected by User Intermediate Certifica Content Certificate
	* •
	< Back Finish Cancel

6. Click OK button and your Installation is completed.



2.4 How to get Digital ID....

2.4.1 Downloading and Importing a Digital ID

You can also search in the public directory for someone's Digital ID, when you find it, you have to download the ID and import it to your contacts list. If you want to search for someone's Digital ID in public directory please do the following steps:

1. Visit http://www.yatanarponca.com.mm or http://www.yantanarponca.com.mm/reposity and follow the instructions to search for, then select and download the Digital ID.

2. When asked to choose the format for downloading select "someone else's Digital ID for Microsoft IE (4.0 or later) / Outlook Express / Microsoft Outlook (2003/2007) / (Window Live Mail)

3. Click the Download button and save the certificate file on your PC.

2.5 Importing Digital ID to Contacts

To import a downloaded Digital ID into your Contacts:

🖹 New Message
<u>File E</u> dit <u>V</u> iew Insert F <u>o</u> rmat <u>T</u> ools <u>M</u> essage <u>H</u> elp
🛤 Send 🔏 🛍 🗎 🏷 🍰 🧩 🖉 🔞 👪 🖛 🛤 🛤
ा To: <mark>[nilataye@myanmat.cnm.mm≤nilataye@myanmat.cnm.mm≥</mark> ;]
Type recipients' names, separated by semicolons or commas
Subject:
▼ E, B / U A, 日日律律 ■ = = = = ● M
*
9

- 1. When you send an email to recipient, Double click on recipient email(red mark).
- 2. Select IDs tab and click Import button.
- 3. Then choose recipient public key and click OK.

ummary	Name and E-mail	Home	Work	Family	Notes	IDs)			
S <u>e</u> lec	t an e-mail addre	ss:								
nilar	aye@myanmar.c	om.mm						•		
<u>D</u> igita	al IDs associated	with the s	selected	d <mark>e-mai</mark> l	addres	5				
									P <u>r</u> operties	
									Remo <u>v</u> e	
									Set Preferred	
								_		
	mport	E <u>x</u> port						•		
What	: is a digital ID?									

3. Certificate Application

3.1 Signing Individual E-Mail

You can automatically sign all your outgoing E-mail by using your Digital ID installed in your browser or E-mail application. Signed E-mail lets the E-mail recipients to verify your identity.

If you want to sign an outgoing message please follow these steps:

1. In the New Message window, click on the Digital Sign message button.

The signed icon will display in the upper right corner of the address pane and it indicates the message is signed or not.

Testing with Digitally sign message	
<u>File E</u> dit <u>V</u> iew Insert F <u>o</u> rmat <u>T</u> ools <u>M</u> essage <u>H</u> elp	
🛤 Send 🔏 🛍 🗎 🏷 🎄 🍄 🕘 🚚 🗮 🖼 🖳	
To: nilaraye@myanmar.com.mm < nilaraye@myanmar.com.mm>;	<u> </u>
E Ca	_9
Subject: Testing with Digitally sign message	_
Arial 10 頁 B / U △, 註 註 律 律 重 幸 書 ■ ─ 劔 🔜	
Hello Dear, i juz testing with Digitally sign message :)	*
Good luck	
	-
	.iti

3.2 Signing All Outgoing E-Mail

To Sign all outgoing message automatically:

- 1. Select the **Tool** menu and scroll to **Option**.
- 2. Select the Security tab and Mark Digital **sign all outgoing messages**.
- 3. If you do not check this box, all outgoing message will not include sign symbol.

and a second second								1	
ieneral	Read	Receipts	Send	Compose	Signatures	Spelling	Security	Connection	Advanced
Virus P	rotectio	on —							10
	Sele	ect the secu	rity zor	e to use:					
			2000	Less secure zone (Moi	e, but more re secure)	functiona	1)		
	V 1	<u>W</u> arn me w	hen oth	er applicat	tions try to :	end mail	as me.		
		Do <u>n</u> ot allo be a virus.	w attacl	nments to I	be saved or	opened th	nat could	potentially	
Downl	oad Ima	ages —							
		<u>B</u> lock imag	es and o	other extern	nal content	in HTML e	-mail.		
Secure	Mail								
	doc		at allow	you to pro	s) are speci ove your ide		Dig	gital IDs]
	To		n mess	ages or rec	eive encryp al ID.	ted	Get	Digital ID]
		Encrypt cor	ntents a	nd attachn	nents for all	outgoing	message	5	-
		Digitally sig	n all ou	tgoing me	ssages				
							Ad	vanced]
							ок	Cancel	Apply

3.3 Individual Encrypting your E-mail

You can also encrypt individual message or configure your e-mail security option to automatically encrypt all E-mail messages to the recipients whose Digital IDs are stored in your contacts list.

3.3.1 Encrypting Individual Messages

To encrypt an outgoing message:

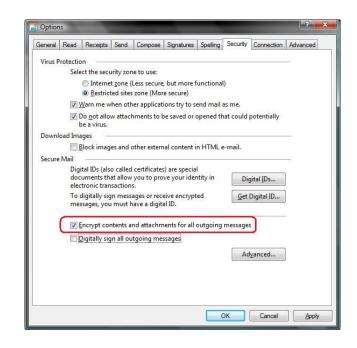
- 1. In the message window click on the **Encrypt Message button**.
- 2. If you do not have recipient's Digital ID, you can't send encrypted message.
- Add the recipient's email address in your contacts and import recipient's certificate in your Contacts List. (See 2.5)

Testing with Encrypt message	
<u>File Edit View Insert Format Iools Message Help</u>	
🛤 Send 🦨 🛍 🖹 🏷 🍰 💯 🖉 👭 🕶 🛤 📑 🖳	
To: nilaraye@myanmar.com.mm < nilaraye@myanmar.com.mm>;	
E Ca	-9
Subject: Testing with Encrypt message	
Arial 10 10 10 10 ↓ 10 ↓ 10 10 0 ↓ 10 10 0 0 0 0 0 0 0 0	
Hello Dear, i juz testing with Encrypt message :)	^
Good luck	
	+
	11

3.3.2 Encrypting All Outgoing E-Mail

You can automatically encrypt all your outgoing email:

- 1. Select the **Tool** button from Menu bar and scroll to Option tab.
- 2. Select **Security tab** and mark the **Encrypt** contents and attachments for all outgoing messages.
- 3. If you mark this message, all your outgoing email will be encrypted.



4. Things to Know...

4.1 How to protect your digital IDs

When private keys are stored in hardware tokens, smart cards, and other hardware devices which are password- or PIN- protected, be sure to use a strong password or PIN. Never give your password to others. You should not write your password down, but if you must, store it in a secure location.

Keep your password strong by following these rules:

1. Use eight or more characters

2. Mix uppercase and lowercase letters with numbers and special characters

3. Choose a password that is difficult to guess or hack, but that you can remember without having to write it down

4. Do not use a correctly spelled word in any language, as these are subject to "dictionary attacks" that can crack this password in minutes

5. Change your password on a regular basis. Contact your system administrator for guidelines on choosing a strong password.

To protect private keys stored in P12 (Portable format for storing/transporting a user's private keys and certificates)/PFX (Personal Information Exchange) files, use a strong password and set your password timeout options appropriately. If using a P12 file to store

private keys that you use for signing, set your password timeout option so that your password is always required (this is the default behavior). If using your P12 file to store private keys that are used to decrypt documents, ensure that there is a backup copy of your private key or P12 file so that you can continue to open encrypted documents should you lose your keys.

4.2 What to do if a digital ID is lost or stolen

If your digital ID was issued by a certificate authority, immediately notify the certificate authority and request the revocation of your certificate. You should also stop using your private key.

4.3 Sharing certificates with others

Your digital ID includes a certificate that others require to validate your digital signature and to encrypt documents for you. If you know that others will need your certificate, you can send it in advance to avoid delays when exchanging secure documents. Businesses that use certificates to identify participants in signing and secure workflows often store certificates on a directory server that participants can search to expand their list of trusted identities.

If you use a third-party security method, you method, you usually don't need to share your certificate with others. Third-party providers may validate identities using other methods, or these validation methods may be integrated with Acrobat. See the documentation for the third-party provider.

When you receive a certificate from someone, their name is add to your list of trusted identities as a contact. Contacts are usually associated with one or more certificates and can be edited, removed, or unassociated with another certificate. If your trust a contact, you can set your trust setting to trust all digital signatures and certified documents created with their certificate.

You can also import certificates from a certificate store, such as the windows certificate store. A certificate store may contain numerous certificates issued by different certification authorities.