YATANARPON TELEPORT COMPANY LTD.,

Yatanarpon Certification Authority

USER MANUAL FOR SECURE E-MAIL MICROSOFT OUTLOOK (2003)

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 E-mail Account in Microsoft Outlook 2003
- 2. Certificate Installation.
 - 2.1 Subscriber/ User certificate installation (PFX)
 - 2.2 CA certificate Installation
 - 2.3 Root certificate Installation
 - 2.4 Get Digital ID
 - 2.4.1 Downloading and Import a Digital ID
 - 2.5 Import Digital ID to Contacts
 - 2.5.1 Importing Digital ID From Trust Center (Default signed Messages)
 - 2.5.2 Importing Digital IDs/Certificates (Proving Identity)
- **3.** Certificate Application.
 - 3.1 Signing individual E-mail
 - 3.2 Signing all outgoing E-mail
 - 3.3 Encrypting your E-mail
 - 3.3.1 Encrypting Individual Messages
 - 3.3.2 Encrypting all outgoing email
- 4. Things to know...
 - 4.1 How to protect your digital IDs
 - 4.2 What to do if a digital ID is lost or stolen
 - 4.3 Sharing certificates with others

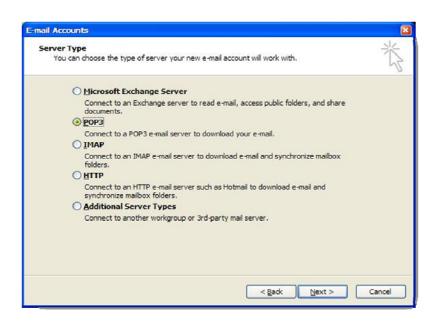
1. Creating E-mail Account in Microsoft Outlook 2003

To configure email account setting in Microsoft Outlook:

- 1. Go to Menu bar and select the **Tools** then scroll down to **Email Account** button.
- 2. Choose Add a new e-mail account and click Next button.

E-mail Accounts		×
	This wizard will allow you to change the e-mail accounts and directories that Outlook uses. E-mail Add a new e-mail accounts View or change existing e-mail accounts Directory Add a new directory or address book View or change existing directories or address books	
	< Back Next > Close	כ

3. Choose **POP3** server type and click **Next** button.

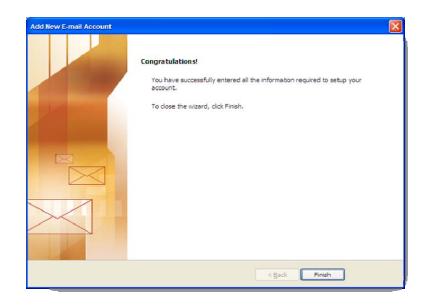


4. In E-Mail dialog box fill the **User Information** and **logon Information** in appropriate boxes. In **logon Information**, please fill the user name from the email address and the password which you use for your email address.

5. In **Server Information**, type the mail server numbers. These numbers (marked with red color) can be changed according to the domain name. Then, click **Next** button.

	ail Settings (POP3) ese settings are required to ge	et your e-mail account working.	×
User Informat	tion	Server Information	
Your Name:	operatingca	Incoming mail server (POP3) 203.81.71.104	
<u>E</u> -mail Address:	operatingca@myanmar.col	Outgoing mail server (SMTP) 203.81.71.114	
Logon Informa	ation	Test Settings	
<u>U</u> ser Name:	operatingca	After filling out the information on this screen, we recommend you test your account by dicking the	
Password:	******	button below. (Requires network connection)	
	Remember password		
Log on using Authenticatio	Secure Password in (SPA)	Test Account Settings	ngs
		< Back Next >	Cancel

6. You will see the following dialog box and Click **Finish.**



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

To use digital ID in your system, you need to install 3 certificate files provided by Yatanarpon CA. They are,

- 1. Subscriber / User Certificate Installation (.PFX) File
- 2. Certification Authority (.CER) File and
- 3. Root Certification Authority (.CER) File

2.1 Subscriber/ User Certificate Installation

- 1. Click your Certificate (.**pfx**) file.
- 2. You will see Certificate Import Wizard and click Next button.
- 3. Specify the file you want to import by clicking **Browse** button and choose your file, then click **Next** button.

e to Import	
Specify the file you want to im	port.
<u>File name:</u>	
or\Desktop\CA\Myanmar_Cer	rtificate\operatingca\operatingca.pfx Browse
Note: More than one certificat	te can be stored in a single file in the following forma
Personal Information Excha	ange-PKCS #12 (.PFX,.P12)
Cryptographic Message Syr	ntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certifica	ate Store (.SST)
	10 - 20 - 10 IS

For the security, the private key is protected with a password.
 Type the password for the private key. Mark all Check boxes and click Next button.

ass	word
T	o maintain security, the private key was protected with a password.
1	ype the password for the private key.
	Password:

	 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.

5. Select **Place all Certificates in the following store** and **click Browse** button then click **Next**.

lificate In	nport Wizard
Certificate	
Certific	ate stores are system areas where certificates are kept.
Window	s can automatically select a certificate store, or you can specify a location for
OP	utomatically select the certificate store based on the type of certificate
⊙ P	lace all certificates in the following store
(Certificate store:
[Browse
	< Back Next > Cance

6. Select the **Personal** Folder and click **OK**. Then click **Next** button in **Certificate Import Wizard** dialog.

elect Certificate Store Select the certificate store you want to use.	? 🛛	tes are kept.
Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers	el	e, or you can specify a location for red on the type of certificate Browse
		: Back Next > Cancel

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

Completing the Certif Wizard You have successfully completed the wizard. You have specified the following set	e Certificate Import
Certificate Store Selected by User Content	Personal Certificate
< Back F	nish Cancel

8. After completing the Certificate Import Wizard, you need to import a new private exchange key. You can set security level (High or Medium).

Importing a net	w private exchange key
	An application is creating a Protected item.
A	CryptoAPI Private Key
	Security level set to Medium Set Security Level
	OK Cancel Details

9. Click Set Security Level button and tick High check box. (If you want to set High security level) and then click Next button.

Importing a new private exchange key		
	Choose a security level appropriate for this item.	
	< Back Next > Cancel	

10. Importing a new private exchange key dialog will appear. Type password and Confirm: password and then click Finish button.

Importing a new private	exchange key	
	Create a password to Create a new passw Password for: Password:	
	Confirm:	<u>Finish</u> Cancel

11. Click **OK** button from the Certificate Import Wizard dialog. You are about to finish the Certificate Installation.



You can set Medium security level too:-

9. Select the **Medium** button and Click **Next** button. (**If you want to set Medium security level**)

Importing a new private exchange key	
	Choose a security level appropriate for this item. High Request my permission with a password when this item is to be used. Medium Request my permission when this item is to be used.
	< Back Next > Cancel

10. To complete the wizard click **Finish** button.

Importing a new private exchange key		
	You have set your security level to medium. A dialog will prompt for your permission when this item is to be used.	
	< Back <u>Finish</u> Cancel	

11. Click **OK** button and you Finish Certificate installation.

Certifica	te Import Wizard 🛛 🔀
(j)	The import was successful.
	ОК

2.1 CA certificate Installation (.CER)

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

- 1. Click require (MET.cer) file.
- 2. Click Install Certificate button.

Certificate Information This certificate is intended for the following purpose(s): Ensures the identity of a remote computer Proves your identity to a remote computer Protects 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	rtificate	?
This certificate is intended for the following purpose(s): •Ensures the identity of a remote computer •Proves your identity to a remote computer •Ensures software 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	Seneral Details Certification Path	
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	Certificate Information	
•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	This certificate is intended for the following purpose(s):	-
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		•
•Protects e-mail messages •Allows data to be signed with the current time Issued to: MET Issued by: myanmar infotech rootca	•Ensures software came from software publisher	
Issued to: MET Issued by: myanmar infotech rootca	Protects e-mail messages	
The second se	Issued to: MET	-
The second se		
	Issued by: myanmar infotech rootca	
Valid from 3/9/2009 to 3/9/2012	Valid from 3/9/2009 to 3/9/2012	
Install Certificate	Install Certificate	nt
ОК		ĸ

3. Select **Place all Certificate in the following store** button from the Certificate Import Wizard window , click **Browse** button and then Click **Next** button.

	te Store
Certif	cate stores are system areas where certificates are kept.
Windo	ws can automatically select a certificate store, or you can specify a location for
C	Automatically select the certificate store based on the type of certificate
۲	Place all certificates in the following store
	Certificate store:
	Browse
	< Back Next > Can
	<back next=""> Can</back>

4. Select the **Intermediate Certification Authorities** and click **OK** button click **Next** button in **Certificate Import Wizard** status window.

Select Certificate Store	
Select the certificate store you want to use	t <mark>es are kept.</mark>
Personal Trusted Root Certification Authori Enterprise Trust Intermediate Certification Authori Trusted Publishers Untrusted Certificates Show physical stores	ed on the type of certificate
	Cancel

5. The certificate Import Wizard is completed and Click Finish button.



6. The Import was successful and Click **OK** button.



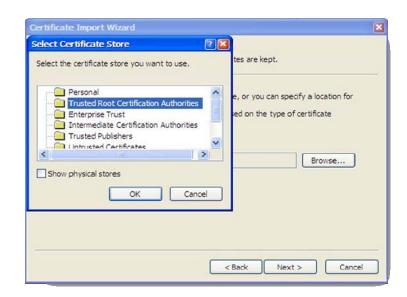
2.2 Root Certificate Installation (.Cer) File

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

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



 Select Place all Certificate in the following store button from the Certificate Import Wizard dialog and click Browse button. You will see the Select Certificate Store Dialog and choose Trusted Root Certification Authorities and Click Next >.



4. After selecting **Trusted Root Certification Authorities** tab from Select Certificate Store dialog you will see again Certificate Import Wizard window as follow and click **Next** button

ertificate Store			
Certificate stores are system a	areas where certificates ar	e kept.	
Windows can automatically sel	ect a certificate store, or	you can specify a	location for
O Automatically select the	certificate store based on	the type of certif	icate
Place all certificates in the second seco	he following store		
Certificate store:			
Trusted Root Certifica	tion Authorities	E	rowse
1			

5. Certificate Import wizard is completed by clicking **Finish** button.

Certificate Import Wizard	Completing the Certifi Wizard You have successfully completed the wizard. You have specified the following setti	Certificate Import
2	Certificate Store Selected by User Content	Trusted Root Certific Certificate

6. Click **OK** button and then your Installation is completed.

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

2.3 Get Digital ID

2.3.1 Downloading and Importing a Digital ID

You can also search public directory for someone's Digital ID, download the ID, and import it to your address book. To search for someone's Digital ID in public directory:

- Visit <u>http://www.yadanarponca.com.mm</u> or <u>http://www.yandarponca.com.mm/reposity</u> and follow the instructions to search for, select and download a Digital ID.
- 2. When the browser asks to choose the format for downloading select "someone's Digital ID" for Microsoft IE (4.0 or later) / Outlook Express / Microsoft Outlook (2003/2007).
- 3. Click the Download button and save the certificate to a file on your PC.

2.4 Import Digital ID to Contacts

To import a downloaded Digital ID into your address book:

1. Open Microsoft Outlook and in the Menu bar, click **Go** button and scroll down to **Contacts** button.

Se operatingca - Cont	lact			
Eile Edit View In	nsert Format Tools Actions Heip			
Save and Close	🗃 🛯 🚩 🤣 🔂 🕲 • + • • •			
General Details	Activities Certificates All Fields			
Full Name	Nilar Aye		E-mail	nilaraye@myanmar.com.mm
Job title:	Test	3	Display as:	nilaraye(nilaraye@myanmar.com.mm)
Company:	Test	<u> </u>	Web page address:	
File as:	Ni lar Aye 💌		IM address:	
Phone numbers	1			
Business				<u>(3)</u>
Home				
Business Fax				
Mobile				
Addresses				
Business				
This is the mailing				

- 2. Select **New**, type the required data in the text boxes.
- 3. After filling the require information click the **Certificate** tab.

🚰 operatingca - Contact	
Elle Edit View Insert Format Iools Actions Help	
🗄 Save and Close 🛃 🖂 🧃 🕈 🌮 🤣 🕲 🔹 🔺 🔹 🕫 🗧	
General Details Activities Certificates All Fields	
Outlook will use one of these certificates to send encrypted mail to this contact. You can get a certificate by receiving digitally signed mail from this contact or by importing a certificate file for this contact.	
Certificates (Digital IDs):	
	Properties
	Set as Default
	Import
	Export
	Remove

4. Click on the **Import** button and choose your file from your computer.

5. Locate the Digital ID you just downloaded and click **Open** button. Then Click on **Save and Close** button.

Two types of Importing Digital ID

2.4.1 Importing Your Digital ID From Trust Center(Default Signing Messages)

When you finish configuring your email setting, you need to import your Digital ID to security option;

- 1. Go to Menu bar click **Tools** Menu and scroll down to **Options** tab.
- 2. And choose **Security** tab and mark all check box under Encrypted e-mail, (All outgoing messages will be include signed & encrypted message) {see- under 3. Certificate Application.}
- 3. Click **Settings** button.

references	s Mail Se	etup Mail	Format	Spelling	Security	Other	
Encrypted	e-mail			22403			
0	Encry	pt contents	and atta	chments	for outgoir	ng mess	ages
A	Add d	ligital signat	ure to ou	Itgoing m	essages		
	Send .	dear text s	igned me	ssage wh	en sending	signed	messages
	Reque	est S/MIME	receipt fo	or all S/MI	ME signed	messag	es
	Default S	ettina:					Settings
							2c to igain
Security Z					versee.		20032
		zones allow can be run i				cripts an	d active
	Zone:	(S) Rest	icted site	es.	~	Zone S	ettings
Download	Pictures						
	Chan	ge Automat	ic Downlo	ad Settin	05		
	- inching		ie bornine		<u>y</u> s		
		ates) —					
Digital IDs							
	Digital ID:	s or Certific			ts that allo	w you ta	o prove your
	Digital ID:			ions.		_	
	Digital ID:	s or Certific				_	o prove your
	Digital ID:	s or Certific		ions.		_	

After Clicking Settings from Option dialog,

- 1. You will see **Change Security Settings** wizard as follow, then type display name in **Security Settings Name:** .
- 2. Mark both **Default Security Setting for this cryptographic message format** and **Default Security Setting for all cryptographic messages.**
- 3. Click **Choose** button from Signing Certificate:

curity Setting Preference	s	
Security Settings Name		
My S/MIME Settings (a	operatingca@myanmar.com.mm)	1
Cryptography Format:	S/MIME	~
	ting for this cryptographic message format y Setting for all cryptographic messages . New Delete Passwor	
Hash <u>A</u> lgorithm:	SHA1	
	Choose	
Encryption Certificate:		
Encryption Certificate: Encryption Algorithm:	3DES	

4. Choose your file and click **OK** button.

MET Code Signin None 2/4/2011

5. When you finished filling Change Security Settings, click OK.

My S/MIME Settings (o	operatingca@myanmar.com.mm)	
Cryptography Format:	S/MIME	
Security Labels	New Delete Pas	sswor
tificates and Algorithms Signing Certificate:		hoose
		noose
Signing Certificate:	operatingca	hoose hoose

2.4.2 Importing Digital IDs/ Certificates (Proving Identity)

- 1. Go to Menu bar click **Tools** Menu and scroll down to **Options** tab.
- 2. And choose **Security** tab and mark all check box under Encrypted e-mail, (All outgoing messages will be include signed & encrypted message) {see- under 3. Certificate Application.}
- 3. Click Import/Export button from Digital IDs (Certificates) under Security tab.

Preferences	Mai Se	etup	Mail Forr	nat	Spelling	Securit	ty O	ther	
Encrypted	e-mai								
2-	Encrypt contents and attachments for outgoing messages								
~	Add digital signature to outgoing messages								
	Send	dear	text signe	ed me	essage wi	nen seno	ting sig	ned	messages
	✓ Reque	est S,	MIME rec	eipt f	for all S/M	IME sign	ied me	ssag	es
	Defaut S	ettn	p:					V	Settings
Security Z	ones			_	_	_	_	_	_
			allow you e run in HT				r script	ts an	d active
	Zone:	0	Restricte	d sit	es	~	Zo	ne S	ettings
Download	Pictures								
	Chang	je Au	tomatic D	own	oad Setti	ngs	1		
Digital IDs	(Certifica	tec)							
	Digital ID	s or C	ertificate tronic trai			nts that a	alow y	icu ta	prove your
				(import/i	Export		<u>G</u> et a	Digital ID

4. Click **Browse** button from **Import existing Digital ID from a file** and choose our certificate security information file from your locate file.

Locate Security	Profile		? 🛛
Look in:	🛅 test		👻 🕲 • 🖄 🗙 📷 •
My Recent Documents Desktop My Computer My Network Places	(Speritinga		
	File <u>n</u> ame: Files of <u>t</u> ype:	Security Information	v v
Tools 🔹			Open Cancel

5. Type certificate password in **Password**: box and type digital ID name in **Digital ID Name:** box. Check again your password and digital ID then click **OK** button

Import/Export Digit	al ID	X
	Digital ID from a file ID from the file to your computer. You mu ered while exporting the certificate to this	
Import <u>Fi</u> le:	C:\Documents and Settings\Administrat	Browse
Password:	•••••	
Digital ID Name:	Operating CA	
 Export your Digital I this information. Digital ID: 	tal ID to a file ID information into a file. Enter a passwor	rd to help protect
Eilename:		Browse
Passwo <u>r</u> d:		bromocini
⊆onfirm:		
Microsoft Inter	net Explorer 4.0 Compatible (low-security D from system)
	ОК	Cancel

6. If you see again Trust Center status. Please click **OK** button.

3. <u>Certificate Application</u>

3.1 Signing individual E-Mail

You can automatically sign all your outgoing E-mail using your Digital ID installed in your browser or E-mail application. Signed E-mail allows an E-mail recipient to verify your identity.

To Sign an outgoing message:

1. Click <u>New</u> button from Standard menu.

👔 Test - Message				
Eile Edit View Ins	ert F <u>o</u> rmat <u>T</u> ools T <u>a</u> ble <u>y</u>	<u>W</u> indow <u>H</u> elp	Type a question for help	• ×
	V 😼 ! 🕴 💌 🙆 🗉) Options + HTML	- 🔁 🔤	
To <u>nilaraye@</u>	myanmar.com.mm;			
@ Cc		3	35	
Subject: Test		Sign	Button	
B 3 X 5 8	Arial 📉 🔽 10 👻 🛓	• B I U	■■ 三 三 (年 (年	1
Hello				^
	al outgoing signed message.			
				~

2. Click on the Digital **Sign** message ¹ button.

The signed icon will be displayed in the upper right corner of the address pane. It indicates that the message has signed.

3.2 Signing All Outgoing E-Mail.

To Sign an outgoing message automatically, you already mark Add digital signature to outgoing messages check box.

Test - Me	ssage	- 2
Eile Edit	<u>View Insert Format Tools Table Window H</u> elp Type a question for help	• ×
🗄 🖃 Send 📔 🧃) 🔹 🛄 🌡 🖉 🕴 🗮 🎽 😰 🔛 Options 🔹 HTML 🛛 💌 🔛	
🛄 то	nilaraye@myanmar.com.mm;	
💷 Cc		
Subject:	Test	
	Arial ● 10 ● A ● B I 型 ■ 書 書 注 注 律 律	*
		>
Hello		III.
Testing (out	tgoing message with signed & encrypted)	*

- 1. Select the **Tools** menu and scroll to **Options** tab.
- 2. Select the Security tab and Mark to "Add digital signature to outgoing messages.
- 3. If you do not check this box, all outgoing message will not include sign symbol.

3.3 Encrypting your E-mail

You can encrypt individual message or configure your e-mail security option to automatically encrypt all me-mail messages to recipients who Digital IDs are store in your address book.

3.3.1 Encrypting Individual Messages

To encrypt an outgoing message:

😰 Test - Message					
Eile Edit Vi	iew Insert Format <u>T</u> ools T <u>a</u> ble <u>W</u> indow <u>H</u> elp	Type a question for help 🔻 🗙			
⊡ <u>S</u> end 🌒	🕶 🛄 🍇 😼 🕴 🕴 🦞 🔛 Options 🔹				
Што	nilaraye@myanmar.com.mm;	-			
🛄 Cc		âg 🔽 🗾			
Subject:	Test E	ncrypt Button			
	Arial 🔹 10 💌 🗛 🔹 🖪 🖊	⊻ <mark>≣</mark> ≣≣ ∐ ⊟ ∰ ∰			
		<u>^</u>			
Hello Testise with T					
I esting with I	ndividual outgoing Encrypted 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.

3.3.2 Encrypting All Outgoing E-Mail

You can automatically encrypt all your outgoing email, You already mark

- Encrypt contents and attachment for outgoing messages check box.
- 1. Select the **Tool** button from Menu bar and scroll to **Options** tab.
- 2. Select the **Security** tab and mark the **Encrypt contents and attachments for outgoing message**.

3. If you mark this message, all your outgoing email will be encrypted.

{see image -3.1}

4. Things to know...

4.3 How to protect your digital IDs

When private keys are stored on hardware tokens, smart cards, and other hardware devices that are password- or PIN- protected, be sure to use a strong password or PIN. Never divulge 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 these 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.

4.4 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.

4.5 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 thirdparty 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.