USER GUIDE

TCS-CA

Outlook Express Configuration

[VERSION 1.0]

CONTENTS

1 DESCRIPTION

This guide explains the procedure for using the TCS-CA issued digital certificate in Microsoft Outlook Express.

2 OUTLOOK EXPRESS AND CERTIFICATES

Outlook Express supports a standard called Secure Multi-Purpose Internet Mail Extensions (S/MIME), which uses RSA encryption technology. At the core of any S/MIME client, the sender will find support for the Public Key Cryptography Standards (PKCS). S/MIME clients (including Outlook 98 and Netscape Communicator) use the PKCS #7 Cryptographic Message Syntax, which defines the basic structure of the digital signature and envelope.

Note: If the sender has multiple mail accounts configured in his/her Outlook Express, the sender will need a separate certificate for each one because **each certificate is tied to a unique email address**. Outlook Express automatically selects the correct certificate based on the account the sender uses to send messages.

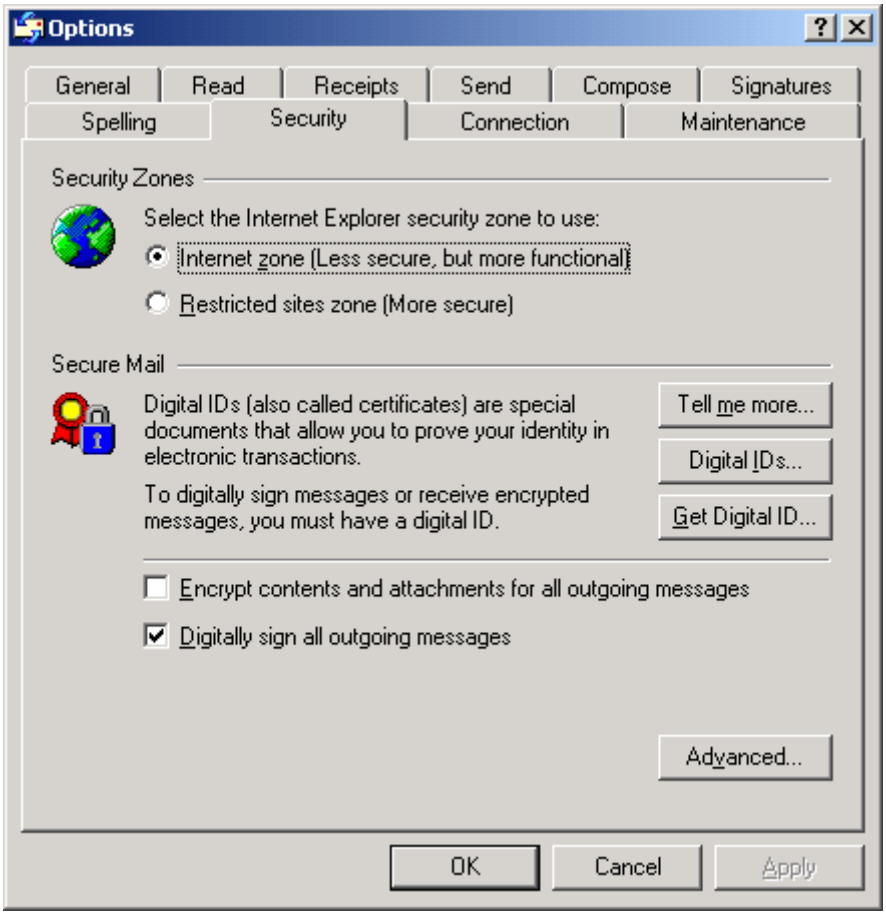
3 ENABLING SECURITY SETTINGS FOR MAIL ACCOUNT

Following steps will enable signing and encrypting all the outgoing messages from the sender's account.

Before that you need to install the required certificates in the IE browser.

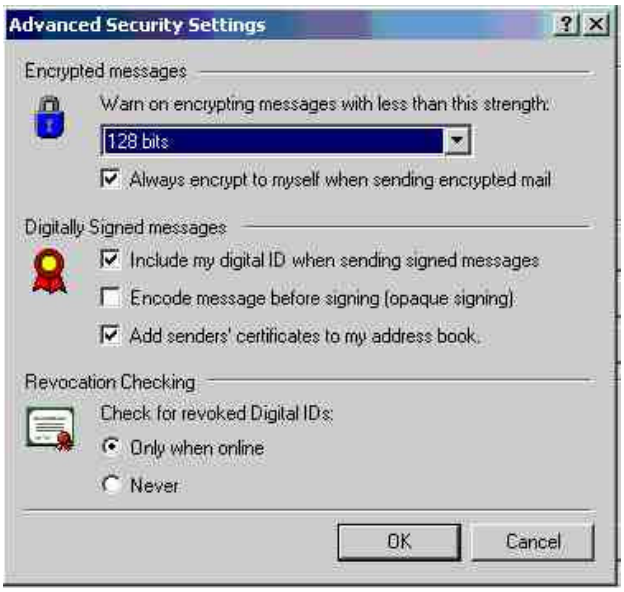
3.1 SETTINGS TO SIGN ALL OUTGOING MESSAGES

1. Select **Options…** from the **Tools** menu.
2. Select the **Security** tab of the **Options** dialog.
3. Check **Digitally sign all outgoing messages** so that it is turned on.
4. Click on **OK** to dismiss the **Options** dialog.



Also enable the option to attach the digital certificate with the outgoing message. This will enable users to verify the message even if they don't have the sender's certificate file. To enable this

1. Select **Options...** from the **Tools** menu.
2. Select the **Security** tab of the **Options** dialog.
3. Click the **Advanced** button in the same dialog box

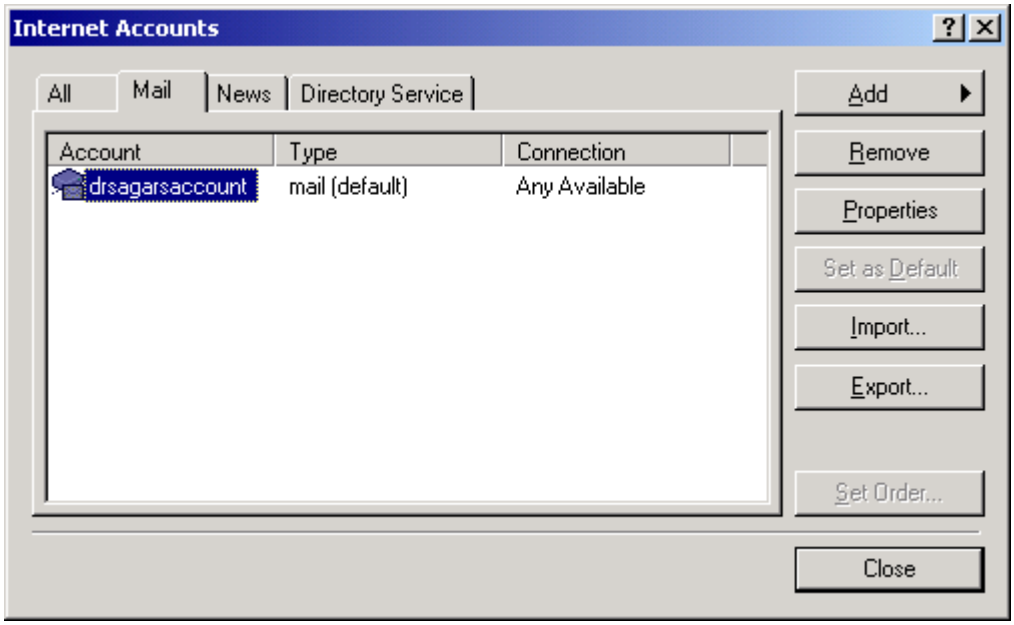


Note: Outlook Express includes the option to digitally sign all the outgoing messages. The sender shall confirm that most of the sender's correspondents use mail software that can accept digital certificates, while configuring this option. For the overwhelming majority of email users, it's best to choose secure email option one message at a time.

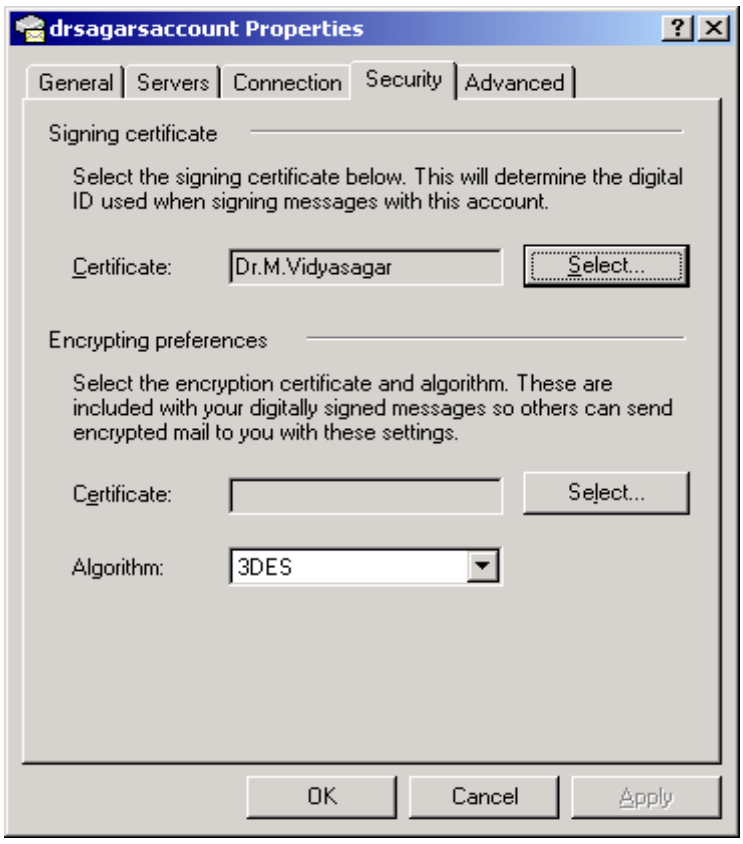
Note: While sending mails if the sender's digital certificate does not exist, Outlook will warn that the message cannot be signed and prompt if the user wants to send an unsigned message instead.

3.2 SETTINGS TO CHOOSE A VALID DIGITAL CERTIFICATE

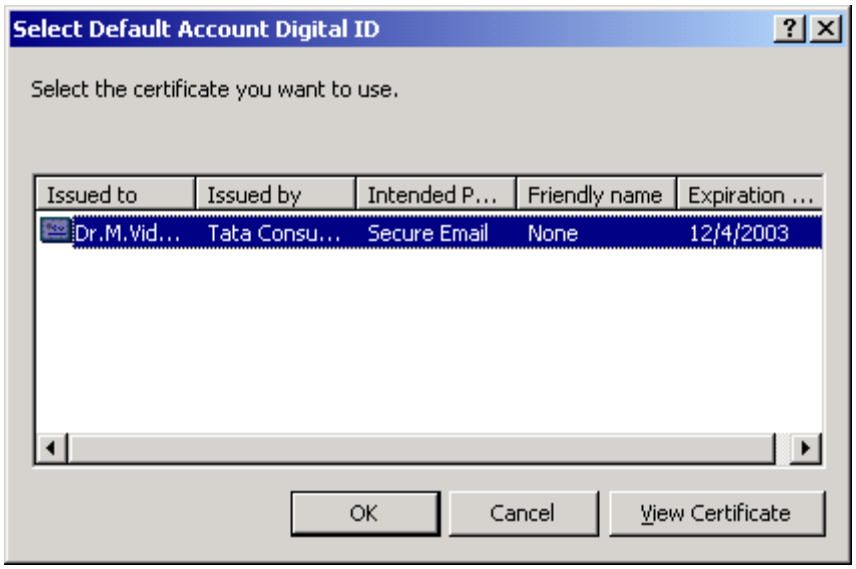
- Select **Accounts...** from the **Tools** menu.
- Select the **Mail** tab of the **Accounts** dialog.



- Select your mails account and select **Properties** for that account for which the sender has obtained Digital Certificate.
- Select the **Security** tab of the **Properties** dialog.



- Click on the **Signing Certificate** - **Select...** button.
- Select the certificate the sender wants to use from the **Select Certificate** dialog, then click on **OK**.



The user's mail account is now configured and ready for use in Outlook Express!

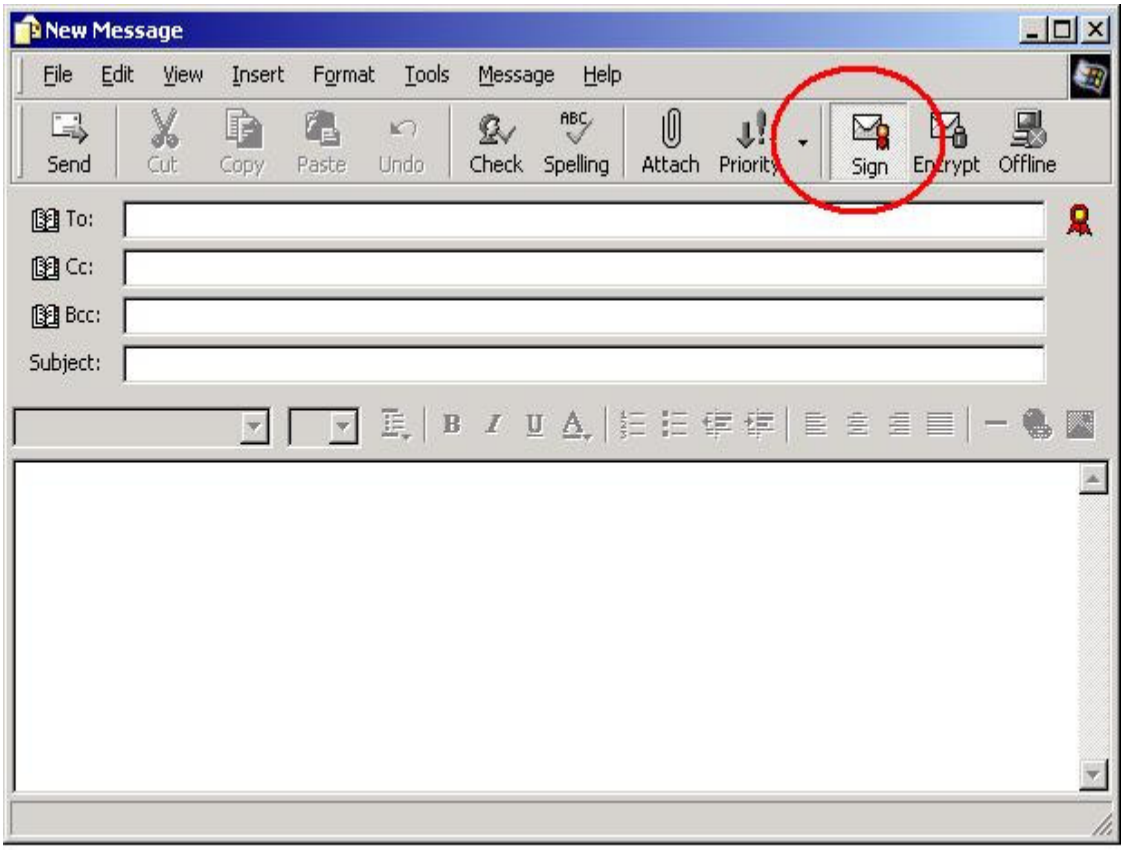
4 SENDING INDIVIDUAL SIGNED OUTGOING MESSAGES

Incase the sender does not want to activate the option to sign and encrypt all outgoing messages but wants to sign certain outgoing messages, it is possible with Outlook Express.

4.1 SENDING SIGNED MESSAGE

The sender has the option of only signing the message to authenticate to the recipient the identity of the sender. Here the private key of the sender is used to sign the message and a copy of the digital certificate (containing the public key of sender) is send along with the message.

- Create a new email by clicking on the **New Mail** button.
- The **New Message** composition window will open.
- Click on the **Sign** button in the menu bar **or** select the **Digitally Sign** item from the **Tools** menu as in the figure.

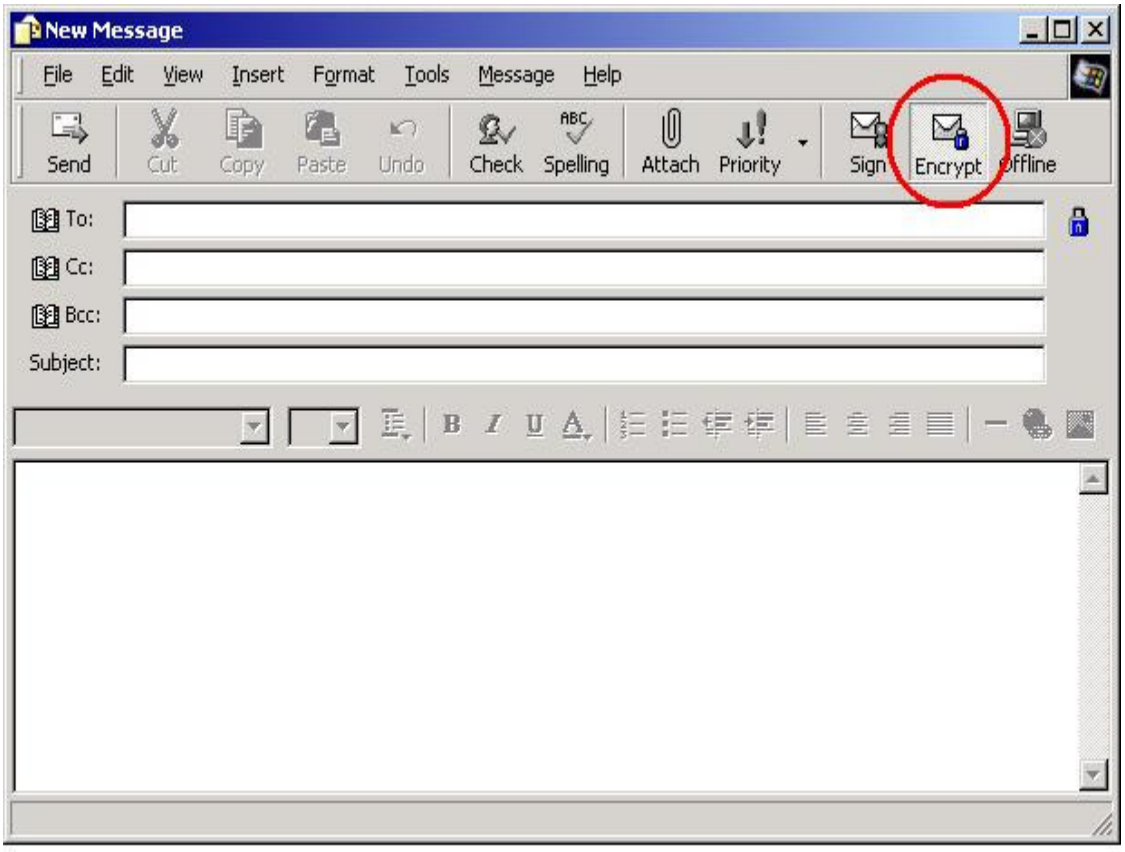


When the sender send a signed email, the sender's private key is used to digitally sign the message. Depending on the private key security level the sender established when the sender first installed the sender's personal digital certificate, when the sender click on the *Send* button, the sender may receive either an **OK/Cancel** prompt or a prompt for the sender's private key password. If the sender selected a private key security level of *"Low",* the message will be sent without warnings or prompts.

4.2 SENDING ENCRYPTED MESSAGE

The sender can send encrypted email to anyone who has a digital certificate. Simply ask the sender's correspondent to send the sender a signed email or the certificate file as an attachment. Once the sender has received a signed email, the sender's email program will store the sender correspondent's digital certificate in the sender's email address book. Once the sender have the other persons digital certificate in the sender's email address book, the sender can encrypt all email to the correspondent by clicking on the encrypt button.

- Create a new email by clicking on the **New Mail** button.
- The **New Message** composition window will open.
- Click on the **Encrypt** button in the menu bar **or** select the **Encrypt** item from the **Tools** menu as shown below.



Note: The sender is only able to encrypt this email if the sender has the public key of the recipient. If the sender attempt to send an encrypted email to someone for whom the sender do not have a public key, Outlook Express will warn the sender that this is not possible and offer the sender the choice of sending unencrypted or not sending.

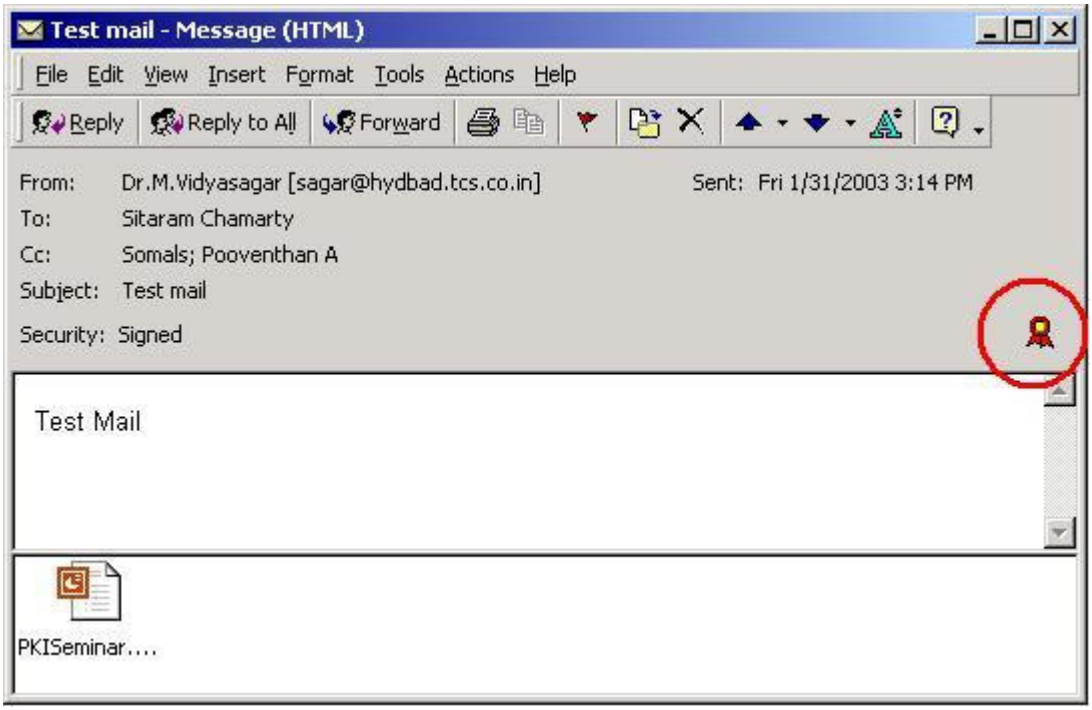
4.3 RECEIVING SIGNED MESSAGE

While receiving signed messaged from others, the receiver can click on the **From** name at the top of the message using the **right mouse button** and can add the other's digital certificate to the address book. When this is done the certificate and

public key information is stored in the address book and you will be now able to send encrypted email to this person.

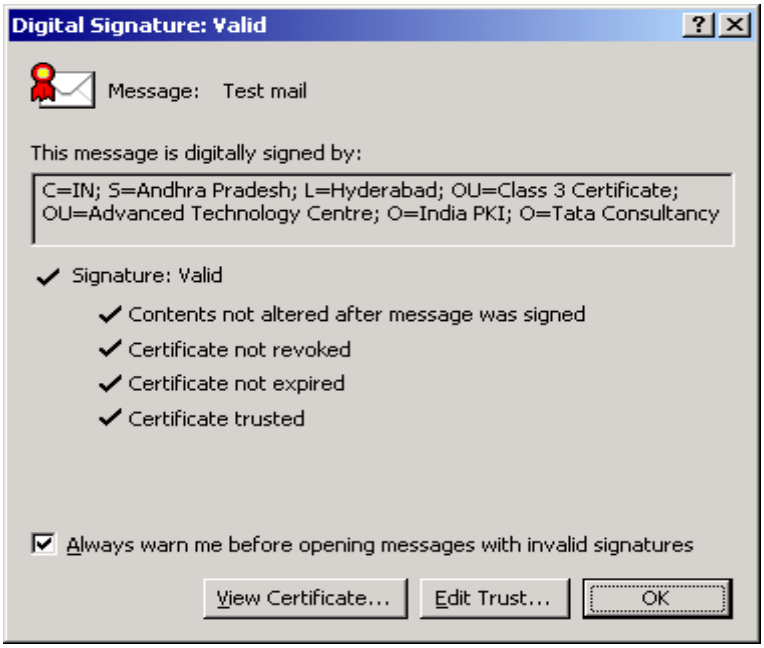
When the user receives a signed message, Outlook Express uses the public key attached with the message to verify the signature.

When the sender receives email, which is signed, and/or encrypted, the message will have the appropriate icon attached to it. The following is a typical signed mail.



The red icon indicates that the message is a signed message.

The blue padlock indicates that it is an encrypted mail. The receiver can click on these icons to examine the details of the certificate used to sign and/or encrypt this message. The following is the screenshot for the signed mail.



5 MANAGING DIGITAL CERTIFICATES WITH OUTLOOK EXPRESS

5.1 STORING A CORRESPONDENT'S DIGITAL CERTIFICATE

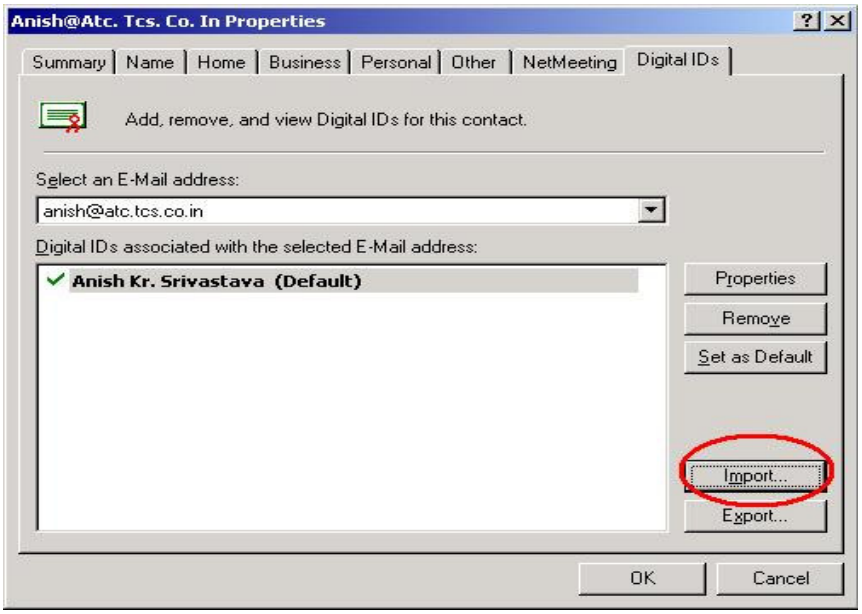
Sending an encrypted message to a correspondent requires the sender to have a copy of their digital certificate. The easiest way to get a copy of someone's digital certificate is to get them to send the sender a digitally signed message incase the encryption and signing certificates are the same. Else he sends the certificate attached to the mail. To store a contact's digital certificate:

- Open the signed message from Outlook Express.
- From the **File** menu select **Properties.**
- Click the **Security** tab.
- Click **View Certificates.**
- Click the **Add to Address Book** button.

5.2 IMPORTING A DIGITAL CERTIFICATE

To import someone's digital certificate that exists in a directory or on the user's hard-drive, download the digital certificate, and add it to the Outlook's address book:

- Select an address
- Choose **File** from the main menu then **Properties**. Click the **Digital Ids** tab.
- Click the **Import** button.
- Search for the digital certificate file and click **Open**.



5.3 TO VIEW A DIGITAL CERTIFICATE

To view details of the digital certificates of recipient

- Open the Address book (**Tools** > **Address Book**) and double click on the correspondent entry that the user would like to view.
- Select the **Digital Ids** tab in the Properties dialog box.
- Select the Digital Certificate that user wants to view and click the **Properties** button.

5.4 TO DELETE A DIGITAL CERTIFICATE FROM THE ADDRESS BOOK

- Open the Address book (**Tools** > **Address Book**) and double click on the entry that the sender would like to view.
- Select the **Digital Ids** tab in the **Properties** dialog box.
- Select the Digital Certificates that user want to remove and click the **Remove** button.

Deleting a correspondent's digital certificate will mean the sender will be no longer able to send encrypted mail to that contact.

CONTACT US

Tata Consultancy Services Limited
[Certifying Authority - PKI Services]
Advanced Technology Centre
Deccanpark, 1 - Software Units Layout
Madhapur, Hyderabad - 500 081

✉ helpdesk@tcs-ca.tcs.co.in
💻 http://www.tcs.com

TATA CONSULTANCY SERVICES