User Guide

May 2013

Using Certificates in Outlook Express

CONTENTS

TABLES

FIGURES

DOCUMENT CONTROL

Title

User Guide - Using Certificates in Outlook Express.

Revision History

Version	Date	Prepared by	Description of revisions
1.0	May 2013		Base Version

Table 1: Revision History

Significant Changes

Document Availability

Soft Form: Soft copy of the document in word format and PDF format would be made available in version control system. This document may be made available in PDF format as part of Dhruvam® deliverable to the customers of Dhruvam®.

ABBREVIATIONS

The following are the abbreviations used in this document.

IE	Internet Explorer
PDF	Portable Document Format
PKCS	Public Key Cryptographic Standards
S/MIME	Secure Multi-Purpose Internet Mail Extensions

Table 2: Abbreviations

1. INTRODUCTION

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

Note: If the sender have 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.

1.1. Purpose

The purpose of the document is to explain the usage of digital certificates in Microsoft Outlook Express.

1.2. Scope

The scope of the document is restricted to usage of digital certificates in Microsoft Outlook Express 6.0. This is an indicative document for configuring Microsoft Outlook Express 6.0. The document may be adopted for higher or lower Microsoft Outlook versions.

2. MAIL ACCOUNT SECURITY SETTINGS

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

Note: To enable signing and encryption, senders account should install the chain certificates in IE browser.

2.1. Sign Outgoing Messages Settings

Outlook Express includes the option to digitally sign all the outgoing messages. This section lists the steps to be followed in order to set the options 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'. Refer *Figure 1: Sign Outgoing Messages*.
4. Click on OK to close the 'Options' dialog.

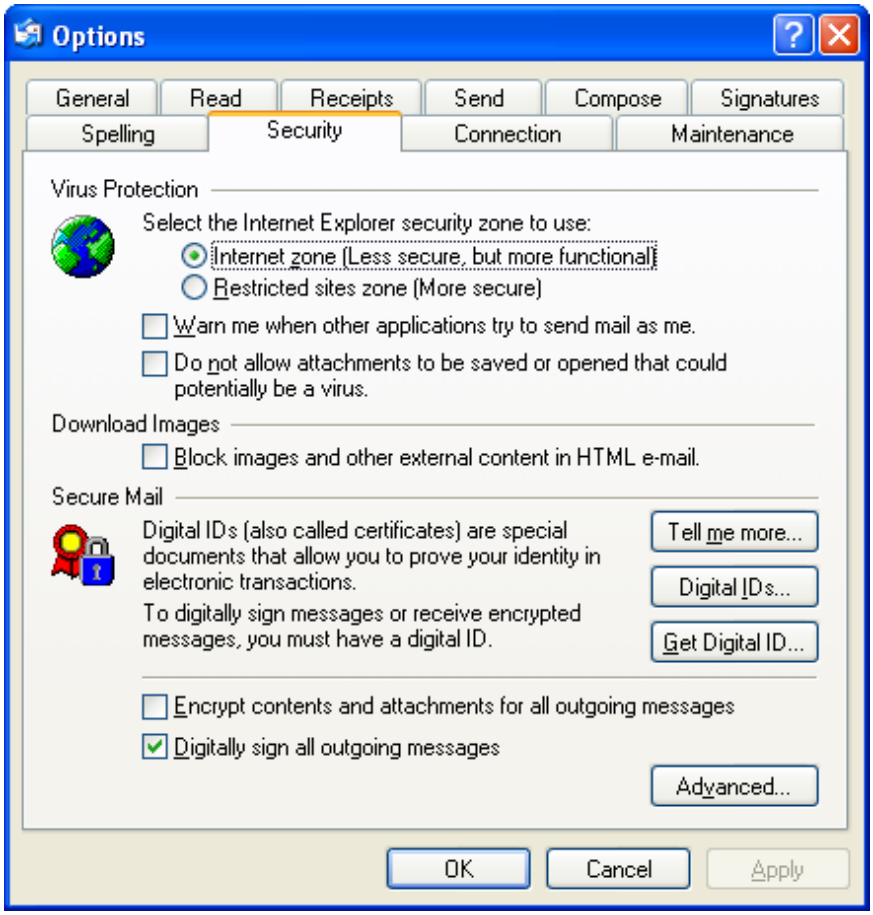

Figure 1: Sign Outgoing Messages

5. Follow the steps below, to enable the option to attach digital certificate with the outgoing message:
    a. Select 'Options…' from the Tools menu.
    b. Select the 'Security' tab of the Options dialog.
    c. Click the 'Advanced' button in the same dialog box. Refer *Figure 2: Advanced Security Settings*.
    d. Check the option, 'Include my digital ID when sending signed messages'.

    By attaching digital certificate with the message, receivers can verify the message even if they don't have the sender's certificate.

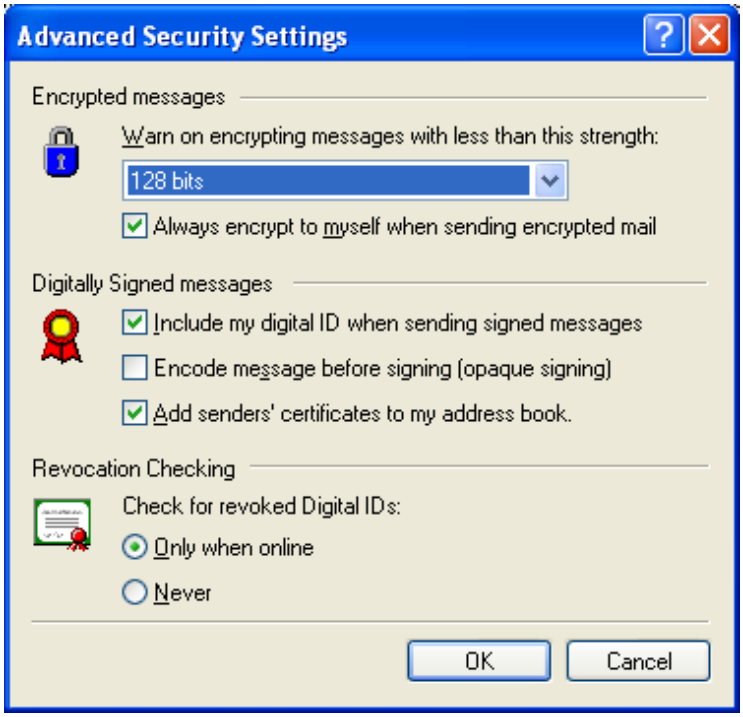

Figure 2: Advanced Security Settings

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.

2.2. Choose Valid Certificates Settings

This section lists the steps to be followed in order to set the options to choose valid certificates.

1. Select 'Internet Accounts…' from the Tools menu. Refer *Figure 3: Internet Accounts.*
2. Select the Mail tab of the Accounts dialog.

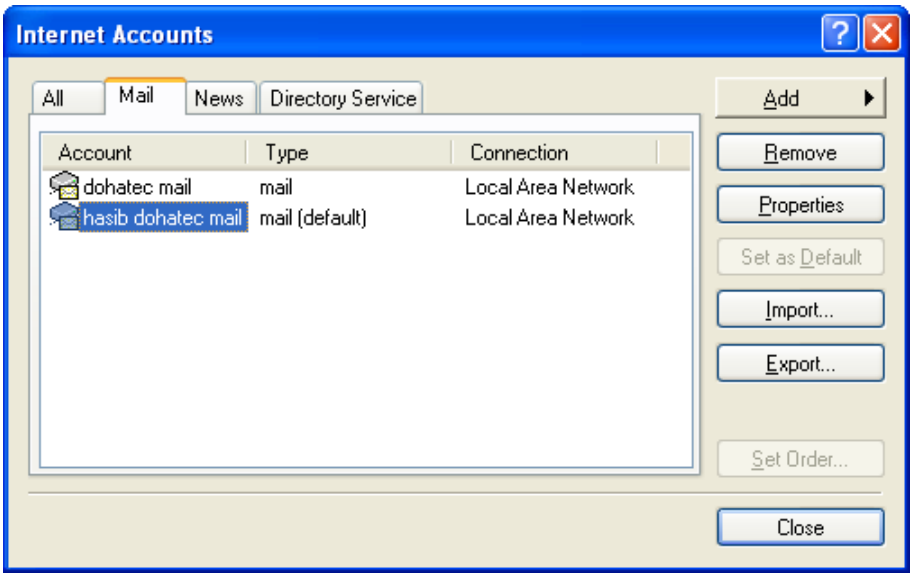

Figure 3: Internet Accounts

3. Select mail account and select 'Properties' for that account for which the sender has obtained Digital Certificate. Refer *Figure 4: Account Properties*.
4. Select the 'Security' tab of the Properties dialog.

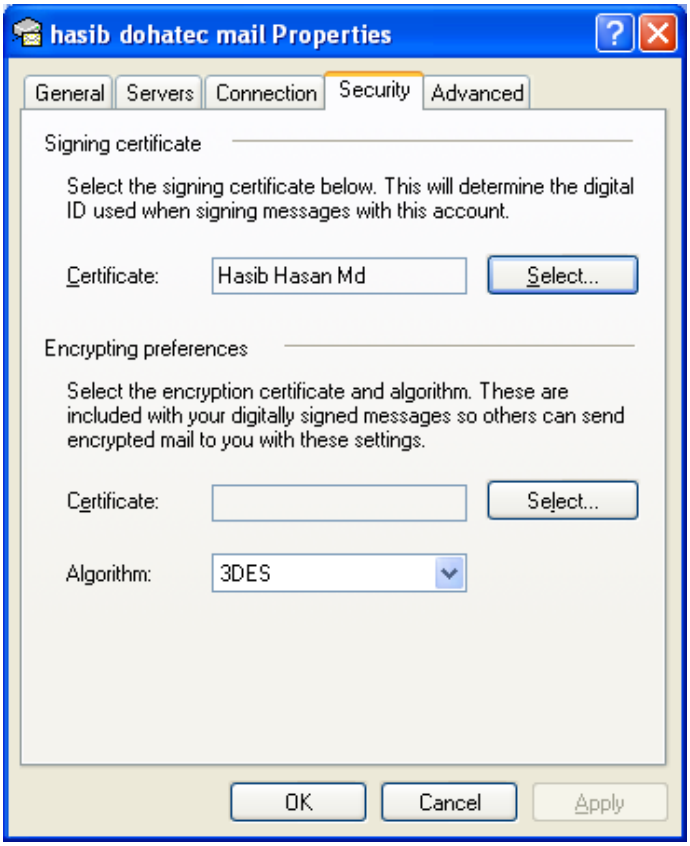

Figure 4: Account Properties

5. Click on the Signing Certificate. Click 'Select…' button.
6. Select the certificate the sender wants to use, then click on OK. Refer *Figure 5: Certificate Selection*.

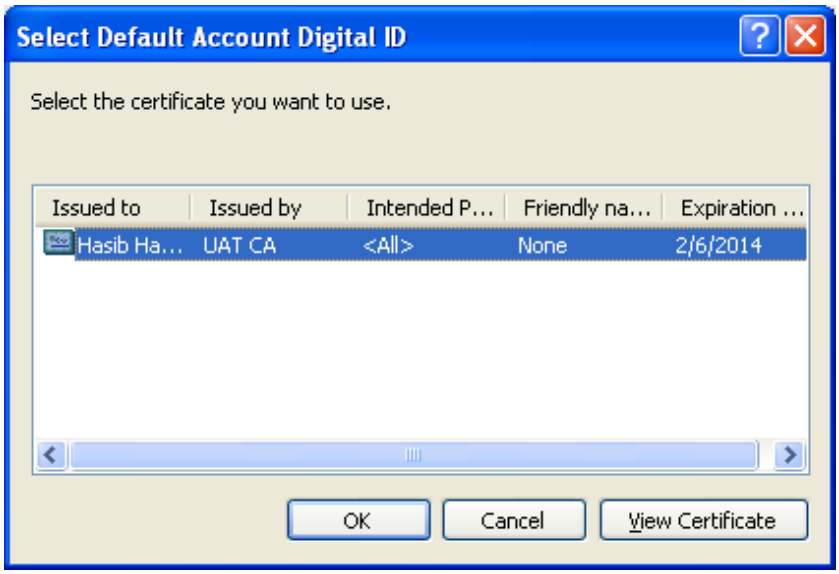

Figure 5: Certificate Selection

3. SIGNED AND ENCRYPTED MESSAGES

The following sections lists the steps to be followed, in case the sender does not want to activate the option to sign and encrypt all outgoing messages but wants to sign certain outgoing messages.

3.1. Send Signed Message

The sender has the option of signing the message to authenticate to the receiver, 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 sent along with the message.

1. Create a new email by clicking on the 'New Mail' button.
2. The 'New Message' composition window will open.
3. Click on the 'Sign' button in the menu bar or select the 'Digitally Sign' item from the Tools menu. Refer *Figure 6: Signing Message*.

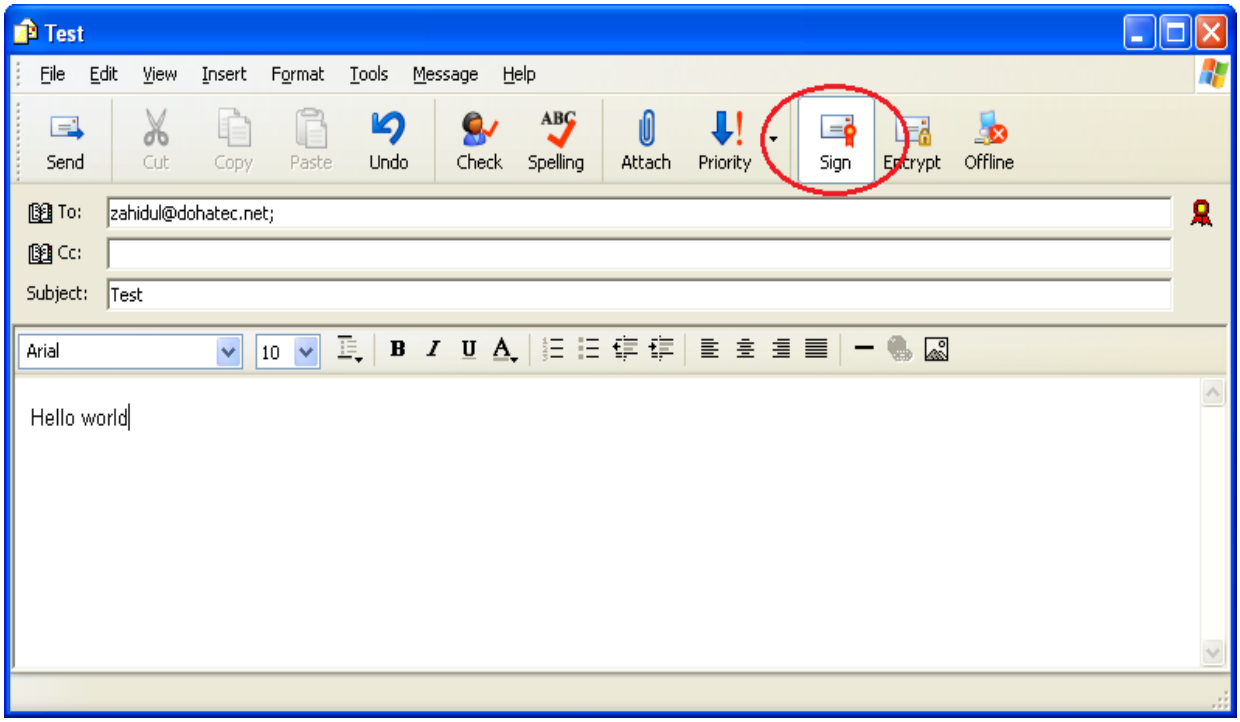

Figure 6: Signing Message

When the sender sends a signed email, the sender's private key is used to digitally sign the message. When the sender clicks 'Send' button, depending on the private key security level, which is established while the sender first installed the sender's personal digital certificate, the sender may receive either an

'OK/Cancel' prompt or a prompt asking 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.

3.2. Send Encrypted Message

The sender can send encrypted email to anyone who has a digital certificate. When the sender's correspondent sends a signed email or the certificate file as an attachment to the sender, the sender's email program will store the correspondent's digital certificate in the sender's email address book.

Once the sender has that correspondent's digital certificate in the sender's email address book, the sender can encrypt all email to the correspondent by clicking on the encrypt button.

1. Create a new email by clicking on the 'New Mail' button.
2. The 'New Message' composition window will open.
3. Click on the 'Encrypt' button in the menu bar or select the Encrypt item from the Tools menus shown below. Refer *Figure 7: Encrypt Message*.

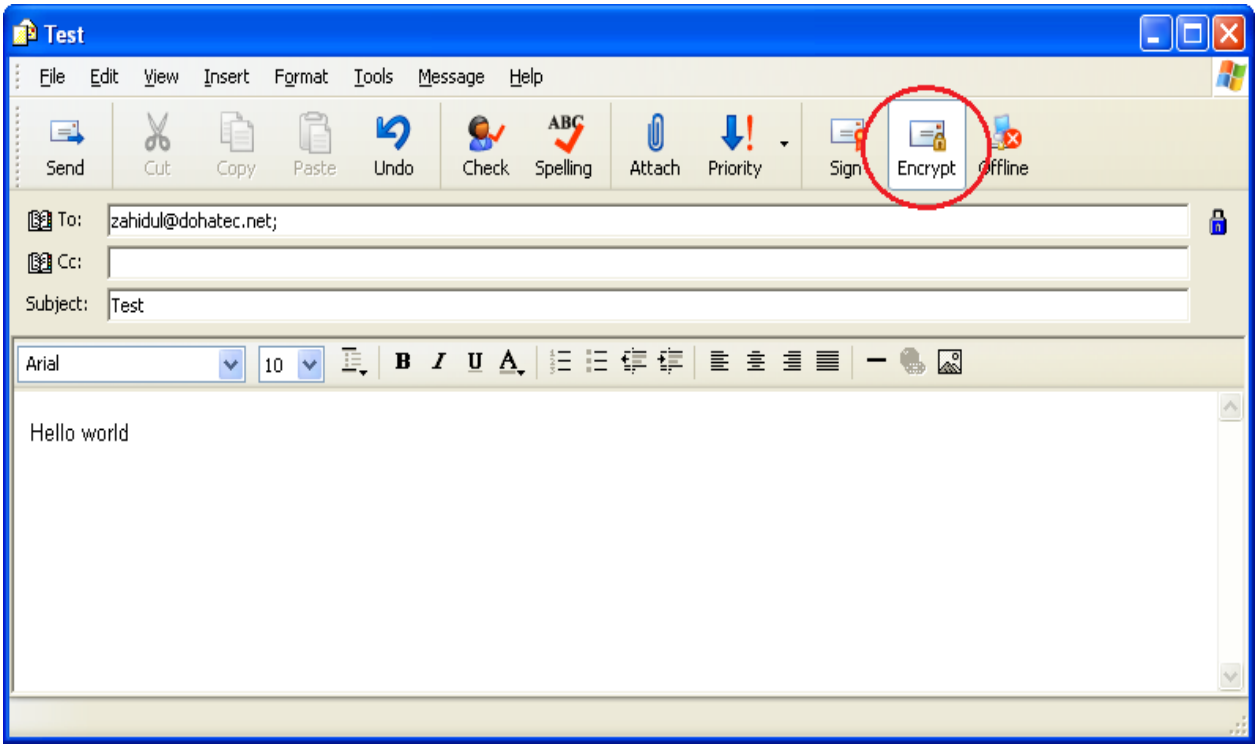

Figure 7: Encrypt Message

The sender is only able to encrypt this email if the sender has the public key of the receiver. If the sender attempts to send an encrypted email to someone for whom the sender does not have a public key, Outlook Express will warn the sender that it is not possible and prompt the sender to send the mail unencrypted or not to send the mail.

3.3. Receive Signed and Encrypted Messages

While receiving signed message from others, the receiver can right click on the 'From' name at the top of the message and can add that particular digital certificate to the address book. When this is done, the certificate and public key information is stored in the address book and the sender 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. Refer *Figure 8: Receive Signed Message*.

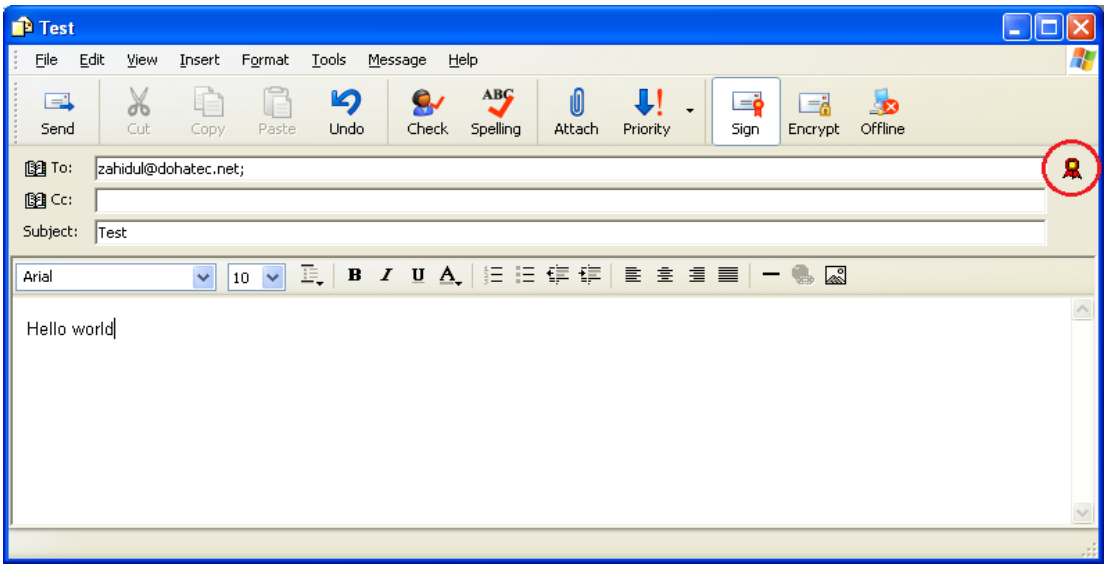

Figure 8: Receive Signed Message

The red icon in *Figure 8: Receive Signed Message* indicates that the message is a signed message.

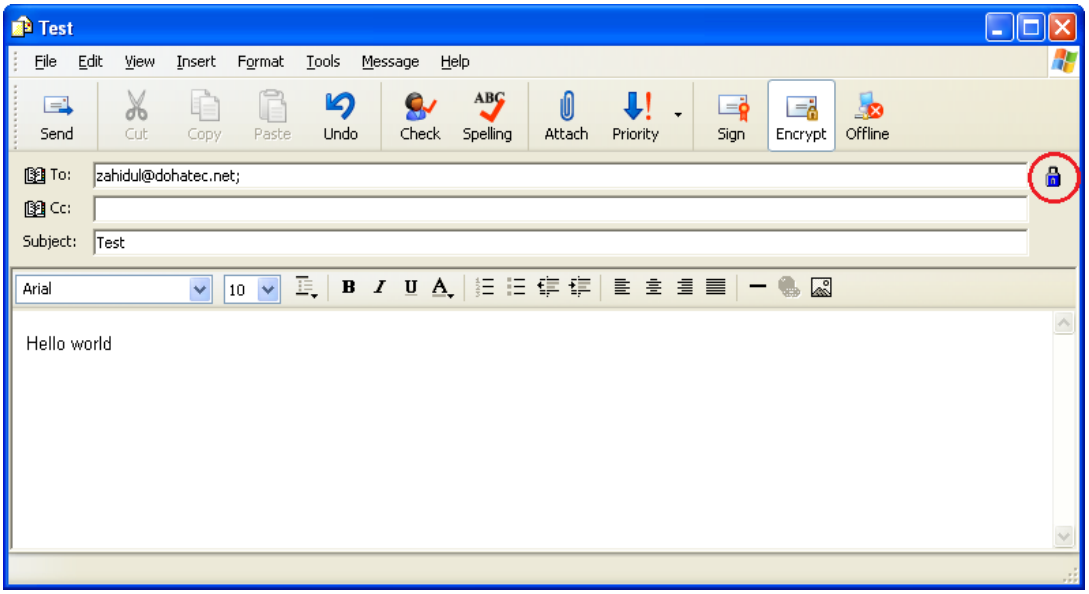

Figure 9: Receiving Encrypted Message

The blue padlock in *Figure 9: Receiving Encrypted Message* 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 the message.

4. MANAGE DIGITAL CERTIFICATES

The following sections provide the information regarding the management of digital certificates with Outlook Express.

4.1. Store 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 the correspondent to send a digitally signed message, in case the encryption and signing certificates are the same. Else the correspondent may send the certificate attached to the mail. To store a contact's digital certificate:

1. Open the signed message from Outlook Express.
2. From the 'File' menu select 'Properties'.
3. Click the 'Security' tab.
4. Click 'View Certificates'.
5. Click the 'Add to Address Book' button.

4.2. Import Digital Certificate

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

1. Select an address
2. Choose 'File' from the main menu then 'Properties'. Click the 'Digital Ids' tab.
3. Click the 'Import' button. Refer *Figure 11: Importing Digital Certificate*.
4. Search for the digital certificate file and click Open.

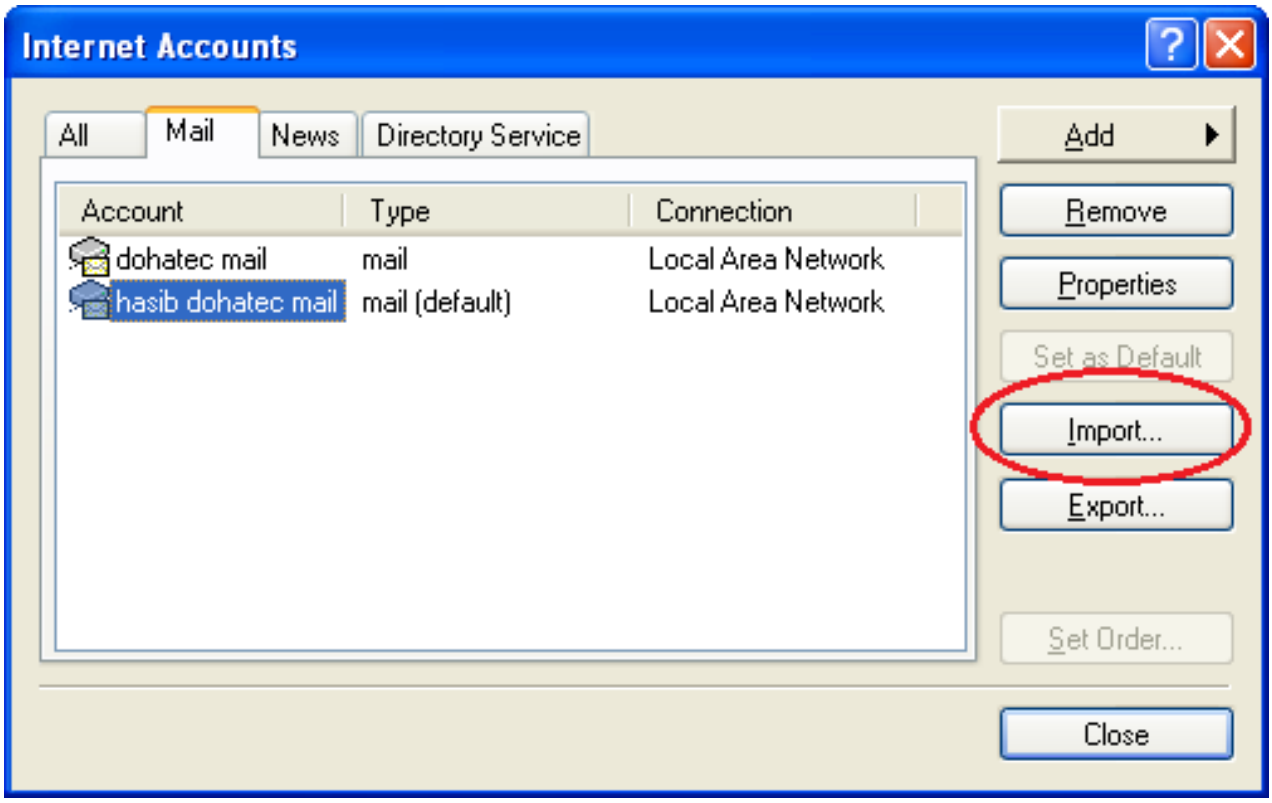

Figure 10: Importing Digital Certificate

4.3. View Digital Certificate

To view details of receiver's digital certificate:

1. Open the 'Address book' (Tools > Address Book) and double click on the correspondent entry.
2. Select the 'Digital Ids' tab in the Properties dialog box.
3. Select the Digital Certificate that user wants to view and click the 'Properties' button.

4.4. Delete Digital Certificate

To delete a digital certificate from address book:

1. Open the 'Address book' (Tools > Address Book) and double click on the entry that the sender would like to view.
2. Select the 'Digital Ids' tab in the 'Properties' dialog box.
3. Select the Digital Certificates that user want to remove and click the 'Remove' button.
4. Deleting a correspondent's digital certificate will mean the sender will be no longer able to send encrypted mail to that contact.