

Solutions for Security

Guide for Securing E-mail With WISeKey CertifyID Personal Digital Certificate (Personal eID)

*Wherever Security relies on Identity,
WISeKey has the solution.*

Date: September 2007
Version: 0.1.0
Authors: WISeKey SA

TABLE OF CONTENTS

About this User Guide	1
<i>About Personal eID (Digital Certificate)</i>	<i>1</i>
<i>About WISEKey Smartcards and USB Tokens</i>	<i>1</i>
<i>Copyright</i>	<i>2</i>
<i>Document Conventions</i>	<i>2</i>
About Digital Signature and Encryption	3
<i>Digital Signature on E-mail</i>	<i>3</i>
Digital Signing Process	3
Signature Verification Process	3
<i>E-mail Encryption</i>	<i>4</i>
Encryption Process	4
Decryption Process	4
<i>Usage of Keys</i>	<i>4</i>
Secure E-mail using WISEKey CertifyID Personal eID	5
<i>Configuring your eID in Microsoft Outlook</i>	<i>5</i>
<i>Sending a Signed Email Message</i>	<i>6</i>
<i>Viewing a Signed Email Message</i>	<i>7</i>
<i>Encrypting an Email Message</i>	<i>10</i>
<i>Viewing an Encrypted Email Message</i>	<i>11</i>
<i>Creating Contacts with Digital Certificates</i>	<i>13</i>
Saving a Contact from the Received Signed Message	13
Creating a Contact with Digital Certificate	14
Support	15

About this User Guide

This manual describes the steps followed for securing your email transactions using WISEKey CertifyID Digital Certificate (eID). It explains the procedure to incorporate your eID in Microsoft Outlook, Outlook Express and Outlook Web Access to send digitally signed and encrypted e-mail messages.

About Personal eID (Digital Certificate)

A digital certificate provides the individual user with the highest level of security; enabling identification, authentication, secure encrypted communications (e-mail, web site etc.), electronic signatures, and non-repudiation.

WISEKey Personal eIDs associate the identity of a person with a digital identity. On one hand a digital ID, or eID can be viewed as Digital Passports that inform Internet users about their interlocutors' identity and ensure electronic messages confidentiality.

Those certificates integrate seamlessly with the majority of existing systems. They are user-friendly, each action being performed via Windows-like active icons.

An eID enables you to:

- Create digital signatures on electronic mail messages, thus ensuring message integrity and authenticity with your correspondents;
- Receive confidential information from any of your correspondents that only you can decrypt and read using S/MIME (You can also send confidential information to other eID users);
- Increase security for your applications, replacing passwords with eID authentication protection (for PKI enabled applications);
- Securely encrypt files and share them with other eID holders using available applications such as the free WISECrypt Personal Edition, available from WISEKey's web site.

About WISEKey Smartcards and USB Tokens

WISEKey provides smartcards, readers, and secure USB tokens for individuals and enterprises. WISEKey smart cards are high quality multipurpose cards that can be used for a variety of purposes including:

- Secure files and documents
- Securely exchange information
- Secure electronic email
- Securely access facilities (wireless proximity access – special version)
- Securely access desktops and servers
- Digital sign documents and files for more efficient electronic workflow and approvals

In addition to signature and PKI applications, and access control systems, the smart card can be used to secure many other sensitive applications, such as payment systems.

Copyright

No part of the contents of this document may be reproduced or distributed in any form or by any means without the prior written permission of WIS@key SA.



is a registered trademark of WIS@key SA.



is a registered trademark of WIS@key SA.

Written and published in Geneva, Switzerland, by WIS@key SA.
Copyright © 2007 WIS@key SA.
All Rights Reserved.

Document Conventions

This User Guide uses the following conventions:

- **NOTE** means *reader take note*. Notes contain helpful suggestions.
- **IMPORTANT** means the reader must follow the instructions strictly.
- Descriptions for significant fields are available.

About Digital Signature and Encryption

Do you write down sensitive data on the back of a postcard? Why not? Because you know, that anyone dealing with the mail underway can read it. The same goes for e-mail, except then it's done electronically in a matter of seconds.

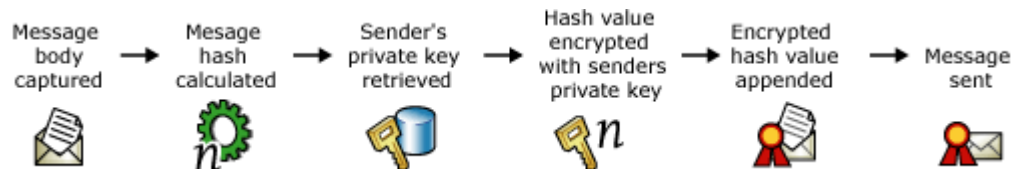
A Public Key Infrastructure is generally considered to be associated with three primary services:

- Authentication - The assurance to one entity that another entity is who he/she/it claims to be.
- Integrity - The assurance to an entity that data has not been altered (intentionally or unintentionally) between "there" and "here," or between "then" and "now."
- Confidentiality - The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.

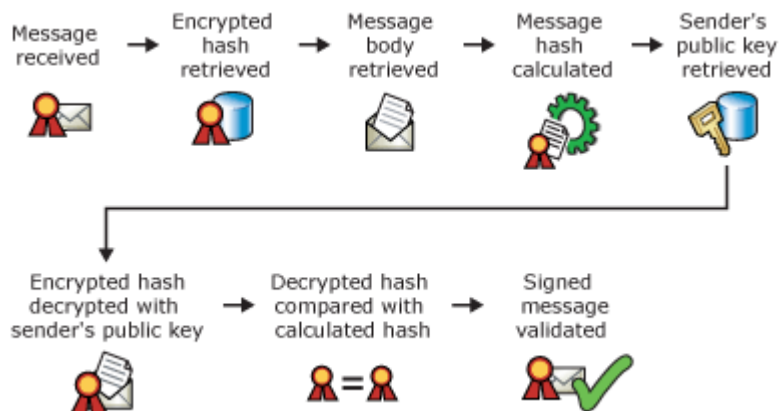
Digital Signature on E-mail

Authenticity may be especially important for business correspondence—if you are relying on someone to provide or verify information; you want to be sure that the information is coming from the correct source. This can be assured using a digital signature on the message. A signed message also indicates that changes have not been made to the content since it was sent; any changes would cause the signature validation to be unsuccessful.

DIGITAL SIGNING PROCESS



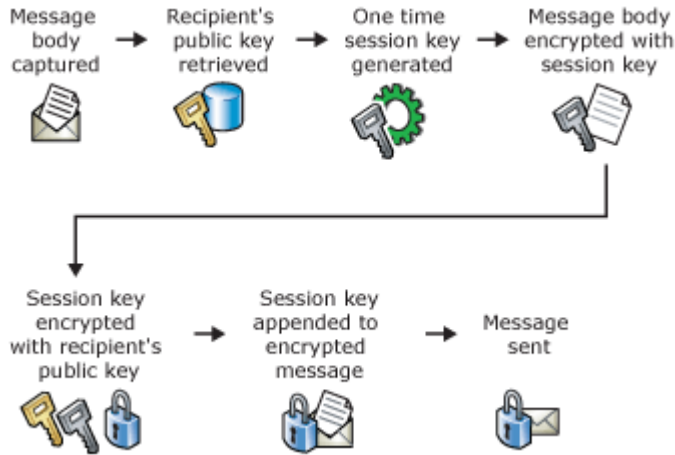
SIGNATURE VERIFICATION PROCESS



E-mail Encryption

One of the main problems with emails is protecting them from being intercepted and read by a hacker. One way of protecting yourself from this is by encrypting your emails. Email encryption means that your email data is scrambled and can only be decrypted through the use of the correct cryptographic key.

ENCRYPTION PROCESS











DECRYPTION PROCESS



Usage of Keys

If someone wants to send you a message that is meant only for you to see, they would encrypt it using your public key. Your private key is required to decrypt such a message, so even if someone intercepted the email it would be useless gibberish to them. When you send an email to someone else you can use your private key to digitally "sign" the message so that the recipient can be sure it came from you by verifying the digital signature with your public key.

	Sender has 	Recipient has 
 Signing	 Sender private key	 Sender public key
 Encrypting	 Recipient public key	 Recipient private key

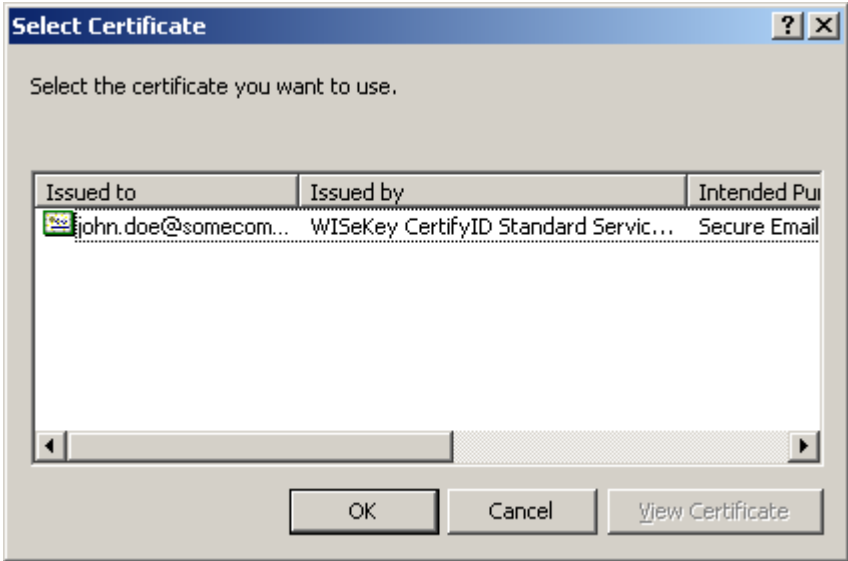
Secure E-mail using WISEKey CertifyID Personal eID

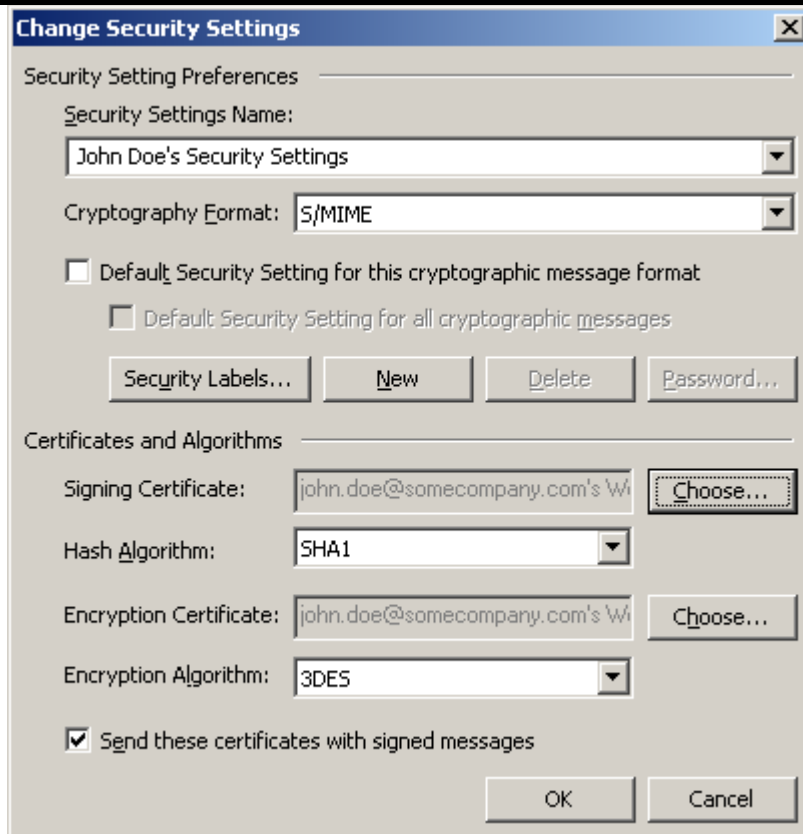
You can secure your email using free WISEKey CertifyID Personal eID. You should obtain your digital certificate (eID) from WISEKey prior to configuring it in your email applications like Microsoft Outlook, Outlook Express or Outlook Web Access. For more information visit <http://www.wisekey.com/>.

Note 1: Obtain digital certificate using an email address that is accessible from an S/MIME capable email application. The email address you submit must be in the exact form as used by your email application, do not use mapped emails. E.g. if your email application accesses your account using john.doe@somecompany.com, then please use this address for getting certificate. Even though jdoe@somecompany.com may be a working alias for john.doe@somecompany.com, it will not work in some S/MIME capable applications.

Important: The root certificates of sender's and receiver's digital certificate should be trusted by the email application or operating system in the sender and receiver's machine prior to configuration.

Configuring your eID in Microsoft Outlook

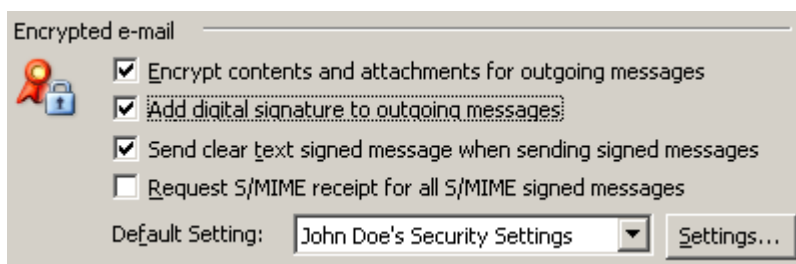
Steps	Instructions
1	Open Microsoft Outlook . Click Tools > Options . Click Security Tab and click Settings button.
2	Click New button in the Change Security Settings dialog.
3	Enter an appropriate name in the Security Settings Name field.
	Click Choose button adjacent to the Signing Certificate field. Select your digital certificate from the Select Certificate dialog box and click OK .
	Click Choose button adjacent to the Encryption Certificate field. Select your digital certificate from the Select Certificate dialog box and click OK .
	Click OK to close the Change Security Settings dialog box.
	



- 4 if you want to sign all the messages that you send by default then in the **Security** Tab, enable the check box **Add digital signature to outgoing messages**.

if you want to encrypt all the messages that you send by default then in the **Security** Tab, enable the check box **Encrypt contents and attachments for outgoing messages**.

Note: It is not recommended to encrypt all messages by default, however signing all messages by default is quite acceptable. You can also decide whether to sign and/or encrypt a message while composing a message.




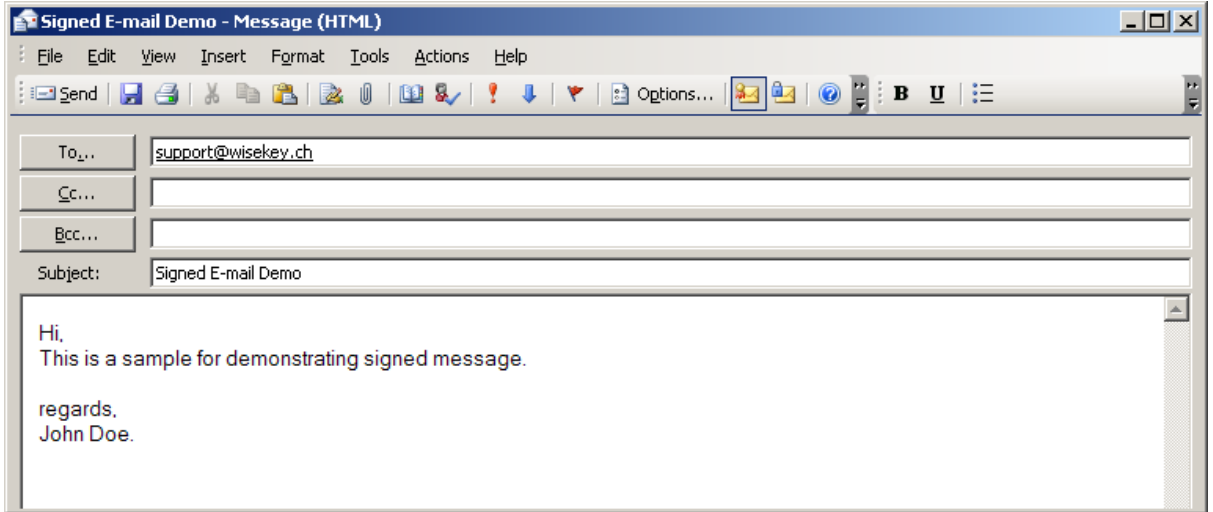
- 5 Click **OK** in the **Options** dialog box to close.

Sending a Signed Email Message

Steps	Instructions
1	Open Microsoft Outlook and compose a new message.
2	Click Options button in the compose message dialog. Click Security Settings... in the Message Options dialog box.

Enable **Add digital signature** to this message checkbox. Click OK. Click **Close** button in **Message Options** dialog box.


Note: Digital Signature on the message can be enabled by clicking  button in the compose message dialog.

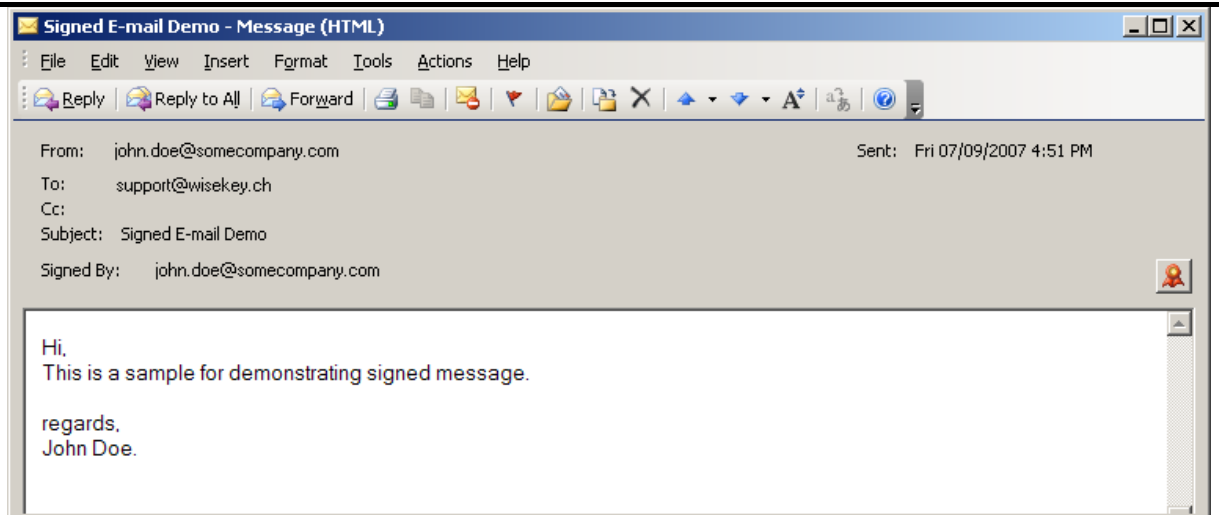


3 Click **Send** button. Your message will be digitally signed and sent to the recipient.

Note: If your key is stored in the smart card, it will prompt for PIN of smart card before sending the message. You should provide the PIN during this process.

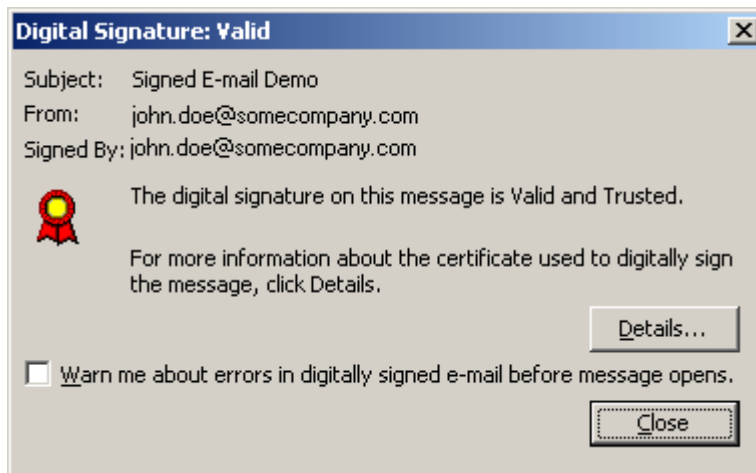
Viewing a Signed Email Message

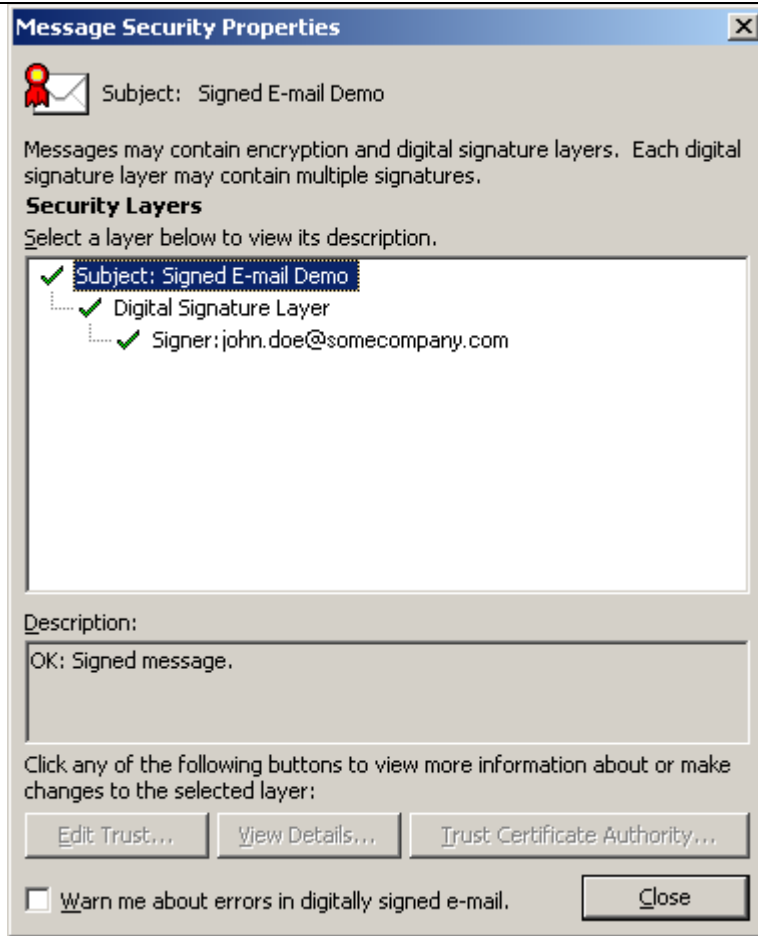
Steps	Instructions
1	<p>Open Microsoft Outlook. Open the signed message you received.</p> <p><i>Note: Microsoft Outlook will verify sender's signature before opening the signed message. Appropriate error messages will be displayed if the signature is not verified.</i></p> 



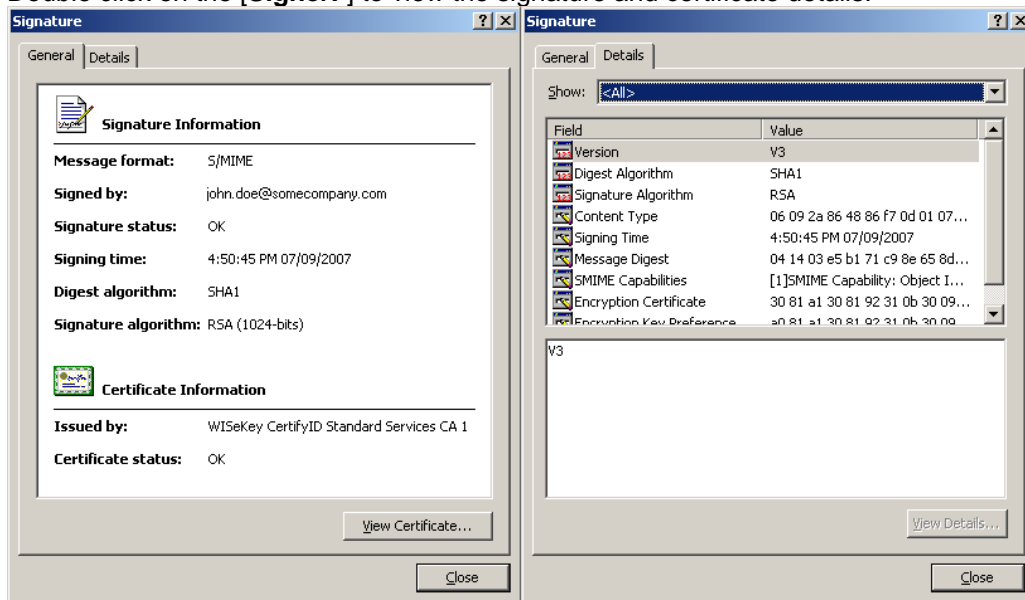
2

Click on the  icon to view the details regarding sender's identity. Click **Details...** button.

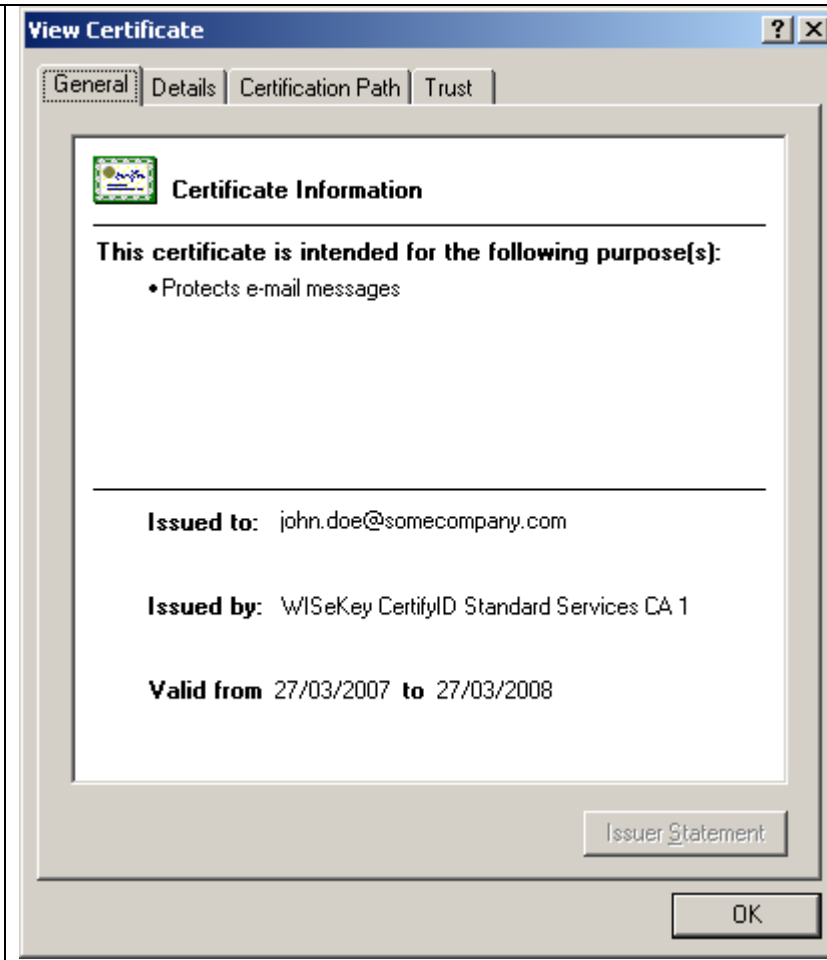




3 Double click on the **[Signer:]** to view the signature and certificate details.




4 Click on **View Certificate...** button in the **General** Tab to view sender's certificate.



Encrypting an Email Message

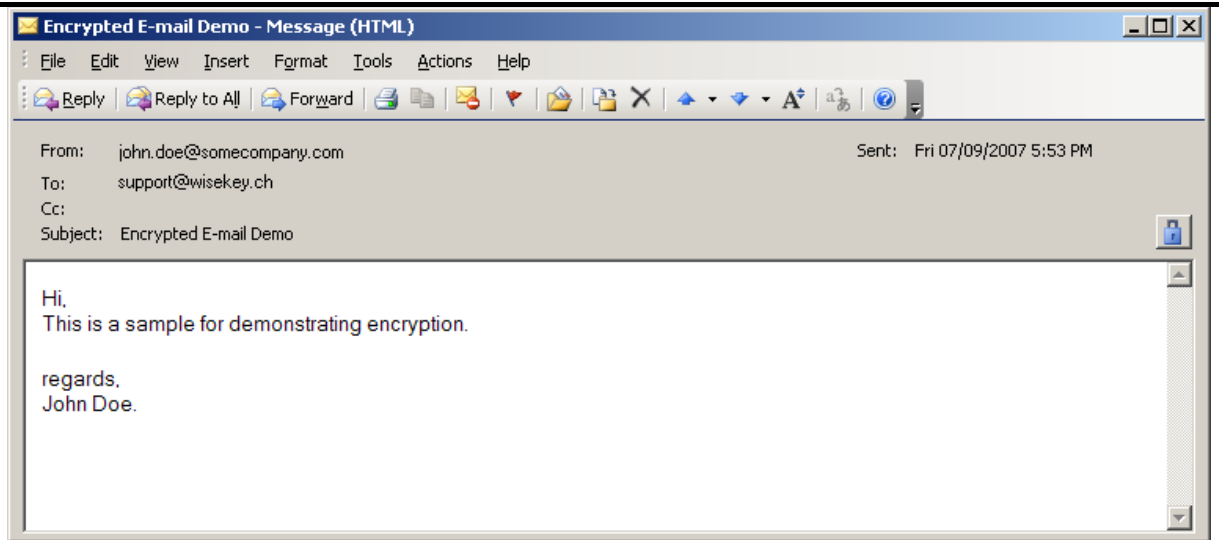
You should have the recipient's public key certificate before encrypting an email. The recipient's digital certificate should be available in Outlook Contacts. If you are sending to a person within your Active Directory domain, the public keys are available automatically. Otherwise, follow the steps mentioned later in the document in section **Creating Contacts with Digital Certificates**.

Steps	Instructions
1	Open Microsoft Outlook and compose a new message.
2	Click the Options button in the compose message dialog. Click Security Settings... in the Message Options dialog box. Enable Encrypt message contents and attachments to this message checkbox. Click OK. Click the Close button in the Message Options dialog box. <i>Note: Encryption on the message can be enabled by clicking  button in the compose message dialog.</i>


3	Click the Send button. Your message will be encrypted and sent to the recipient.

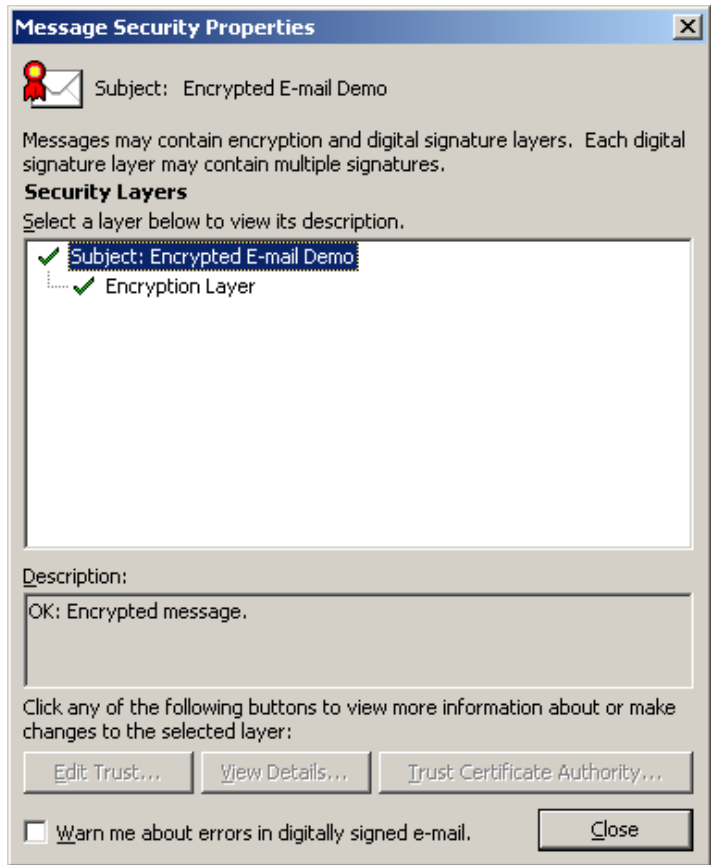
Viewing an Encrypted Email Message

Steps	Instructions
1	<p>Open Microsoft Outlook. Open the signed message you received.</p> <p><i>Note 1: Microsoft Outlook will decrypt the message before opening the encrypted message. Appropriate error messages will be displayed if it is not successful.</i></p> <p><i>Note 2: If your key is stored in the smart card, it will prompt for the PIN of the smart card before decrypting the message. You should provide the PIN during this process.</i></p>



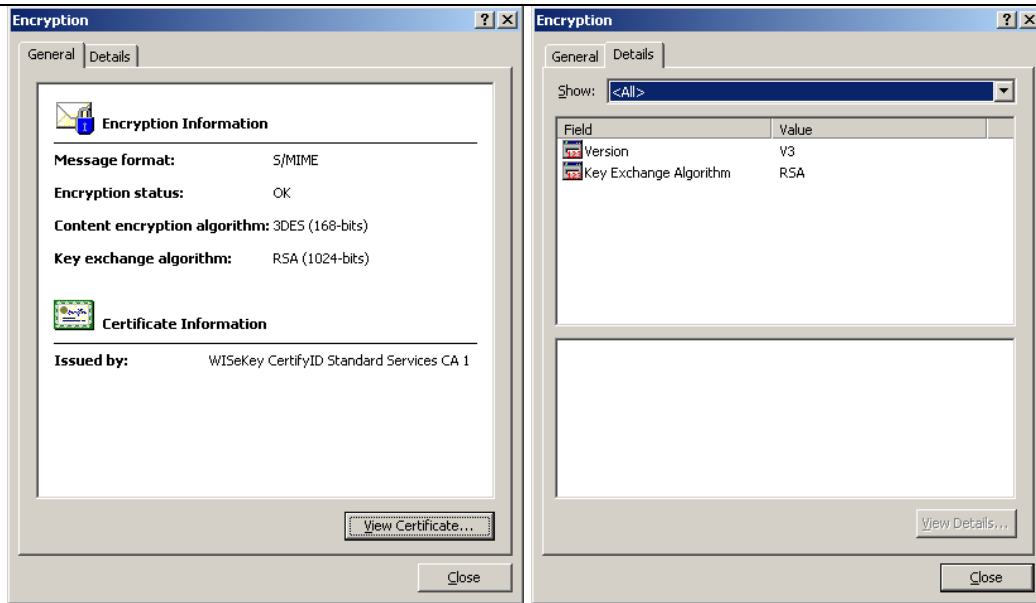
2

Click on the  icon to view the details of the encrypted message.



3

Double click on the **Encryption Layer** to view the encryption and certificate details.



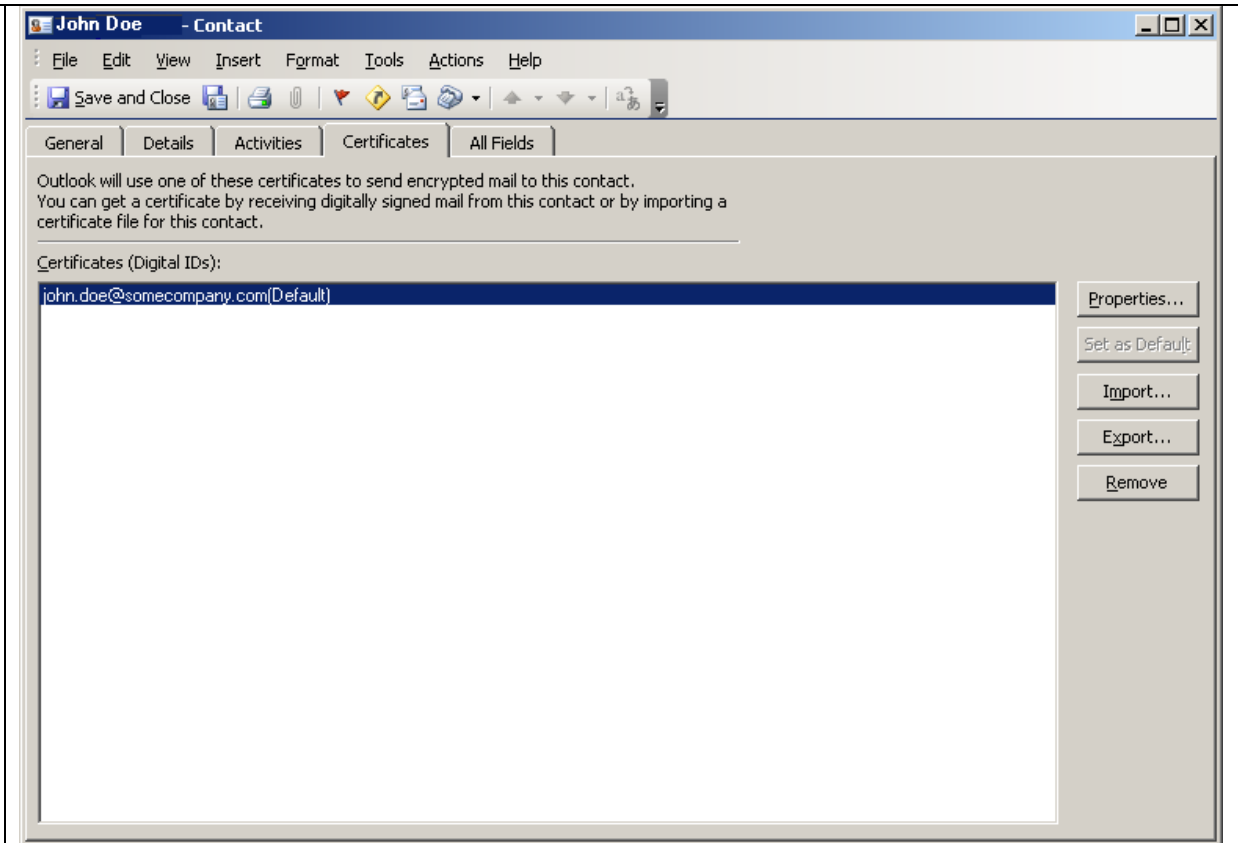
4 Click on **View Certificate...** button in the **General** Tab to view the recipient's certificate.

Creating Contacts with Digital Certificates

To encrypt a message, you need to have the recipient's digital certificate in Outlook Contacts.

SAVING A CONTACT FROM THE RECEIVED SIGNED MESSAGE

Steps	Instructions
1	Open a signed message from the Inbox received by the person whom you want to send encrypted message.
2	Right click on the sender's name in the Sender field. Click Add to Outlook Contacts... menu item. <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> </div>
3	Add necessary details in the General Tab of Contact Dialog. Click the Certificates Tab and check whether the person's certificate is correctly incorporated.




4 Click **Save and Close** button in the **Contact** dialog.

CREATING A CONTACT WITH DIGITAL CERTIFICATE

This procedure can be followed when you don't have a signed message from the person who you want to encrypt message.

Important: You should have the person's encryption certificate with you in DER encoded certificate file.

Steps	Instructions
1	Open Microsoft Outlook and select Contacts . Click New to create a new contact.
2	<p>Add the necessary details in the General Tab of Contact Dialog. Click the Certificates Tab. Click the Import... button. Select the recipient's certificate using File Dialog. Click Yes on the message box.</p> <div data-bbox="288 1554 1501 1765" style="border: 1px solid black; padding: 5px;"> <p>Microsoft Office Outlook</p>  <p>The e-mail address in the certificate is not found in the contact's e-mail list. Do you want to continue to add this certificate into this contact?</p> <p style="text-align: center;"> <input type="button" value="Yes"/> <input type="button" value="No"/> </p> </div>
3	Click the Save and Close button in the Contact dialog.

Support

Should you require support at any stage of this procedure then please contact WISEKey SA :-

WISEKey SA
WTC II / 29 Rte de Pré Bois
Geneva CH-1215
Tel. +41 22 594 3000
Email : support@wisekey.com