



Encrypted Mail User Guide

for Microsoft Outlook Express / Windows Mail

Product Release: 6.5
Release Date: November 16, 2010

Copyright © 2003-2010 Echoworx Corporation
4101 Yonge Street, Suite 708, Toronto, Ontario M2P 1N6 Canada
All rights reserved.

This product or document is distributed under licenses restricting its use, copying, distribution, and decompilation. This document is provided for informational purposes only and Echoworx makes no warranties, either express or implied, in this document. Information in this document, including URL and other internet website references, is subject to change without notice. The entire risk of the use or the results of the use of this document remains with the user.

Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Echoworx Corporation.

Echoworx may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Echoworx, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

About This Guide

This guide describes how to install and use Encrypted Mail with supported Microsoft™ Outlook Express® 6.0 or above and Microsoft™ Windows Mail®.

There are four main sections to the guide:

I) About Encrypted Mail

This includes product information including the system requirements to install and use Encrypted Mail.

II) Getting Started

Step by step instructions on how to download, install and activate the product.

III) Using Encrypted Mail

Here you will find instructions on sending and receiving encrypted messages, accessing tools included with Encrypted Mail, and managing your personal settings.

IV) Support Information

This area of the guide includes frequently asked questions, errors and how to contact us if you have a question, comment or require technical assistance.

There are also two appendixes that contain information relevant to understanding and using Encrypted Mail:

Appendix A: Email Security Concepts and Terminology

This section contains technical concepts and terminology for anyone looking to learn more about identity management, cryptography, PKI and digital certificates.

Appendix B: Privacy Legislation and Encrypted Mail

Included in this section is a brief summary of recently enacted privacy legislation, who is affected and why emails should be encrypted and digitally signed.

Table of Contents

About Encrypted Mail	1
What Defines an encrypted message?	2
Encrypted Mail Components	2
Features and Benefits.....	3
Who Needs Encrypted Mail?.....	4
System Requirements	5
Getting Started	6
Before You Begin	7
Installing Encrypted Mail	8
Activating Your Secure ID.....	13
Validating Your Installation	18
Using Encrypted Mail	19
Sending an Encrypted Message	20
Sending a Digitally Signed Message	22
Setting the Encrypted Mail Reminder Prompt	24
Viewing an encrypted message	25
Encrypted Mail Tools & Settings.....	28
ID & Password Tools	30
Adding a Trusted Contact.....	34
Uninstalling Encrypted Mail	35
Support Information.....	36
Frequently Asked Questions	37
Tips on Creating an Effective Password	41
Known Issues.....	42
Error Messages.....	43
Have a Comment, Question or Need Support?	43
Appendix A: Email Security Concepts and Terminology.....	44
Information Security.....	45
Privacy Versus Security.....	47
Identity Management.....	47
Cryptography	48
PKI and Digital Certificates	50
Appendix B: Privacy Legislation and Encrypted Mail	52
Privacy is Mandated by Law.....	53

About Encrypted Mail

The Threat is Real

We understand the security threats that you face when sending email. Email travels from the sender to the receiver as a virtual postcard, and as email is stored and forwarded through the Internet, there is a real risk that someone other than the sender or the receiver can intercept and either read it or tamper with it.

The content of email is now regularly finding its way into the news or into the hands of people who should not have it. The fact that large volumes of email can be collected, scanned, filtered, read and altered makes email an easier target for illegal interception than regular physical mail. Also, unlike regular mail, you would never know that your email has been intercepted and read or altered.

Encrypted Mail gives you confidence

Encrypted Mail gives you the confidence that only you and your intended recipients are able to read your email, and that you know that the sender is not pretending to be someone else. It's a value added service that gives you the ability to send email with the confidence that the email is securely encrypted and that only the person that you addressed the email to can unlock it. Recipients benefit because the identity of the sender is also guaranteed. With Encrypted Mail, everyone with an email address can send and receive encrypted digitally signed emails, without knowing the details of how it's done.

This section of the guide covers the following topics:

- What Defines an encrypted message?
- Encrypted Mail Components
- Summary of Features and Benefits
- Who Needs Encrypted Mail
- System Requirements

What Defines an encrypted message?

An encrypted message is one that is encrypted, digitally signed, and unalterable.

Encrypted

Your email message and any attachments are garbled and locked up, such that only your intended recipient can unlock and read them.

Signed

When you enter your Encrypted Mail Password, your message is digitally signed to assure the recipient that only you could have sent it.

Unalterable

The contents of your message cannot be altered, so the recipient can be sure that the message they receive from you is genuine.

These qualities assure the sender that only their intended recipient can open and view the message, and the recipient that the message actually came from the purported sender and has not been altered enroute. Subscribers to the Encrypted Mail service never need to worry about the privacy and security of their email messages.

Encrypted Mail Components

Subscribers of the Encrypted Mail service use the following components to send and receive encrypted messages:

Secure ID

Your Secure ID (also known as a digital ID or certificate) is the electronic equivalent of your driver's license or passport. Your ID is associated with your email address and is used to provide proof of your identity when you send Encrypted Mail.

Encrypted Mail Plug-in

Encrypted Mail enables you to send and receive Encrypted Mail messages using your existing email software. Encrypted Mail adds a number of new features to your email software.

Encrypted Mail Password

When you activate Encrypted Mail, you will be asked to create a Secure ID Password. This password should be known only to you, and is used to send and open encrypted messages.

Features and Benefits

Anyone can sign up: you don't need to be a customer to subscribe and can use your existing email address (you@youraddress.com)

Confirm sender's ID: digital signatures guarantee the identity of the sender

Messages are encrypted: military grade security is used to seal your email

Send to anyone: you can send Encrypted Mail to anyone, whether or not they are also a subscriber

Click to send: before sending, just click on the new SECURE button and the email will be encrypted before it is sent from your computer

Click to open: click on an encrypted mail in your email box and enter your password to open it

Managing identities: you don't have to worry about exchanging identities with anyone, just address the email and we do the rest

Truly Secure: trusted standards - public key infrastructure (PKI), digital certificates (X.509), Secure / Multipurpose Internet Mail Extensions (S/MIME)

Economical: one monthly fee lets you send unlimited Encrypted Mail

Who Needs Encrypted Mail?

Consumers care about privacy

Privacy and personal security are two reasons why consumers think twice about sending email. Have you ever decided to pick up the telephone to talk to someone instead of sending them an email because you were concerned that your message could be intercepted? Do you suspect that an email is not actually from the person listed in the "from:" line? Identity thieves and curious people have a growing array of widely available spy-ware and email interception products at their finger tips. Isn't it time to start putting your email into an envelope with a guaranteed return address?

Businesses need trusted communications

Businesses are concerned about ensuring trust in communications, risk to their brand, confidentiality and laws requiring that email be digitally signed and encrypted. Email has become one of the most important and frequently used ways of communicating highly sensitive information. Why is it that businesses continue to risk significant losses by sending email in the clear without digital signatures? The cost of hardware, software, management and training required to build a proprietary encrypted email infrastructure was prohibitively expensive. Today, any business email user can subscribe for a low monthly fee to send unlimited Encrypted Mail.

Encrypted Mail is a valuable tool for businesses in complying with the law. Privacy legislation imposes a general obligation on businesses and government to protect the privacy and security of personal and private information. Some privacy legislation expressly requires that specific measures be taken to protect against unauthorized disclosure of electronically stored or communicated information. Other industry-specific legislation protects the confidentiality and integrity of information relating to specific markets.

Health Insurance Portability and Accountability Act (HIPAA) is an example of legislation that protects personal information sent amongst health care professionals.

Sarbanes-Oxley Act (SOX) governs integrity of financial operations of publicly traded companies.

Gramm-Leach-Bliley Act (GLBA) requires that all financial institutions protect customer information.

California Security Breach Notification Act (CB 1386) requires disclosure when private personal information of a California resident has been compromised.

These are a few important examples of US Federal and State industry-specific legislation that directly or indirectly requires that information contained in email be protected against uncontrolled disclosure, and that requires companies to adopt sufficient measures to ensure integrity and authenticity of private information transmitted electronically.

For more information on recently enacted privacy legislation, who is affected and why emails should be encrypted and digitally signed, please refer to **Appendix B: Privacy Legislation and Encrypted Mail, page 52** of this guide.

System Requirements

The minimum system requirements to install and use Encrypted Mail include:

Operating System
<ul style="list-style-type: none">■ Microsoft™ Windows® 7 32-bit & 64-bit■ Microsoft™ Windows® Vista with Service Pack 2 or higher 32-bit & 64-bit*■ Microsoft™ Windows® XP with Service Pack 3 or higher <p>+ <i>The following applications are not available on 64-bit Operating Systems: Secure File (LOCK files).</i></p> <p>Encrypted Mail for Windows Mail. For Windows 7, Vista and XP, you are required to have administrative privileges.</p>
Email Clients
<ul style="list-style-type: none">■ Microsoft™ Outlook® 2010 32-bit & 64-bit■ Microsoft™ Outlook® 2007■ Microsoft™ Outlook® 2003■ Microsoft™ Outlook® 2002■ Microsoft™ Windows® Mail■ Microsoft™ Outlook Express® 6.0 or above <p>For all other clients we recommend the latest service pack.</p>
Web Browser
<ul style="list-style-type: none">■ Microsoft™ Internet Explorer® 6.0 or above
Internet Connection
<ul style="list-style-type: none">■ Minimum 56 KBPS dial-up modem■ LAN-based using standard TCP/IP■ DSL, ADSL, Cable Modem <p>If you are using a firewall/proxy the client must be able to communicate with the Encrypted Mail application back-end.</p>
Computer Hardware
<ul style="list-style-type: none">■ 5-10 MB of hard drive space■ Pentium 233 MHz (Recommended: Pentium 500MHz or greater)■ 128 MB RAM (Recommended: 256 MB or greater)

Supporting a broad range of system configurations is very important to us. If your system is not currently supported, email info@echoworx.com if wish to receive an alert when Encrypted Mail is ready for your environment.

Getting Started

After completing the account sign-up process, you will be able issue Encrypted Mail licenses to virtually any existing email address. Once an account is established, you will also be able to add Encrypted Mail licenses through the Encrypted Mail portal.

This chapter explains how to install and activate Encrypted Mail after an email has been provisioned through the sign-up or Encrypted Mail portal.

Instructions are included for first-time users, as well as user who are re-installing or installing Encrypted Mail for an activated license on another computer.

This section of the guide covers the following topics:

- Before Your Begin
- Installing Encrypted Mail
- Activating Your Secure ID
- Validating Your Installation

Before You Begin

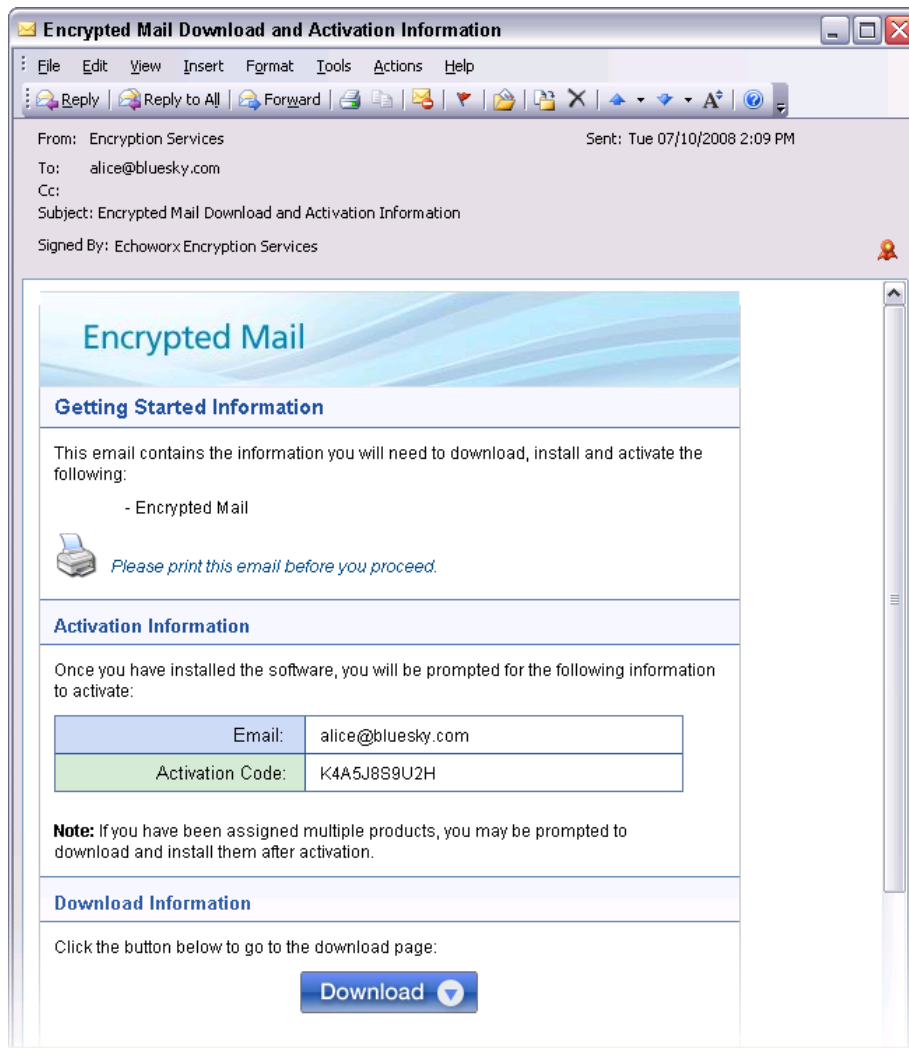
Before you install, you will need the following:

A supported version of Microsoft Outlook Express or Windows Mail (see [System Requirements, page 5](#)).

An existing email address which is properly configured for use in your Microsoft Outlook Express or Windows Mail client (popular webmail accounts such as Hotmail, Yahoo and Gmail can be configured for use in Microsoft Outlook Express and Windows Mail).

For new users, a *Getting Started* email which contains the activation code and a link to download the software (see sample below).

For existing users (reinstalling Encrypted Mail), you will need your Secure ID password.



Installing Encrypted Mail

The *Getting Started* email contains a download link for Encrypted Mail. The download link is also available from the support website.

- 1 To download the program, click the **Download** button located in your 'Getting Started' email.

The Choose Setup Language prompt appears.



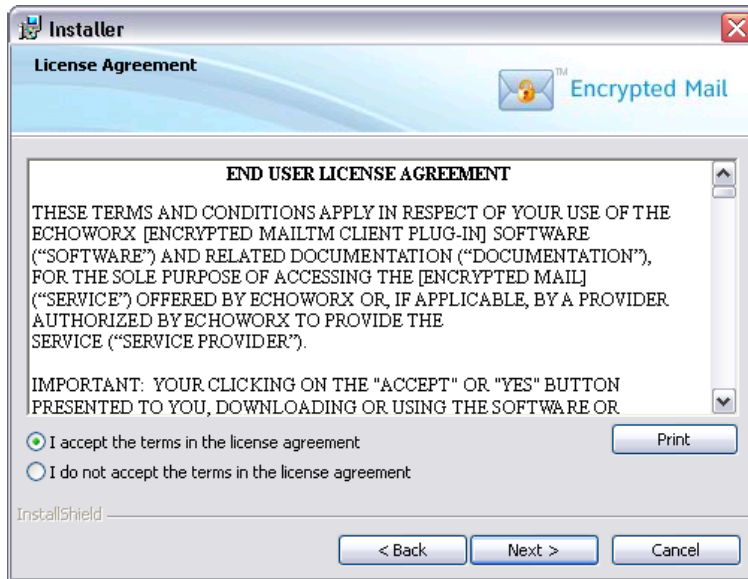
- 2 Using the drop-down menu, select the appropriate installation language and then click **OK**. The Welcome to the Installation Wizard window appears.
- 3 Click **Next**.

At this point, close your email application and any open messages. If you have an email application open, the Files in Use window appears. Close the applications listed in the window and then click **Retry**.

The Welcome to the Encrypted Mail Installer window appears.



- 4 Click **Next**. The End User License Agreement (EULA) window appears.



- 5 If you accept the EULA, select *I accept the terms of the license agreement* and then click **Next**. The Setup Type window appears.



- 6 Choose the setup type for this installation – *Typical* or *Custom*. **Note:** The following describes a *Custom* installation.

- 7 Click **Next**. The Install Type window appears.



- 8 Choose who will have access to this application and then click **Next**. The Destination Folder window appears.

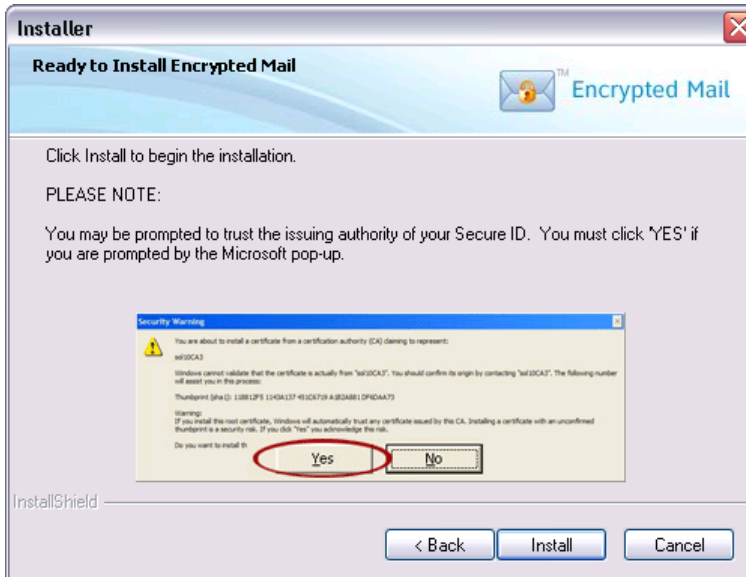


- 9 If necessary, choose a different Destination Folder by clicking **Change...** and selecting an alternate folder. The default Destination Folder is *C:\Program Files\Encryption Services*.

10 Click **Next**. The application selection window appears.



11 Select the options you want to install. By default, all options are selected. Click **Next**. The Ready to Install Encrypted Mail window appears.



12 Read the message and then click **Install**. The *Setup Status* window appears and shows the progress of the installation.

When the installation is complete, the successful installation window appears. The **Activate my software now** checkbox is selected by default.



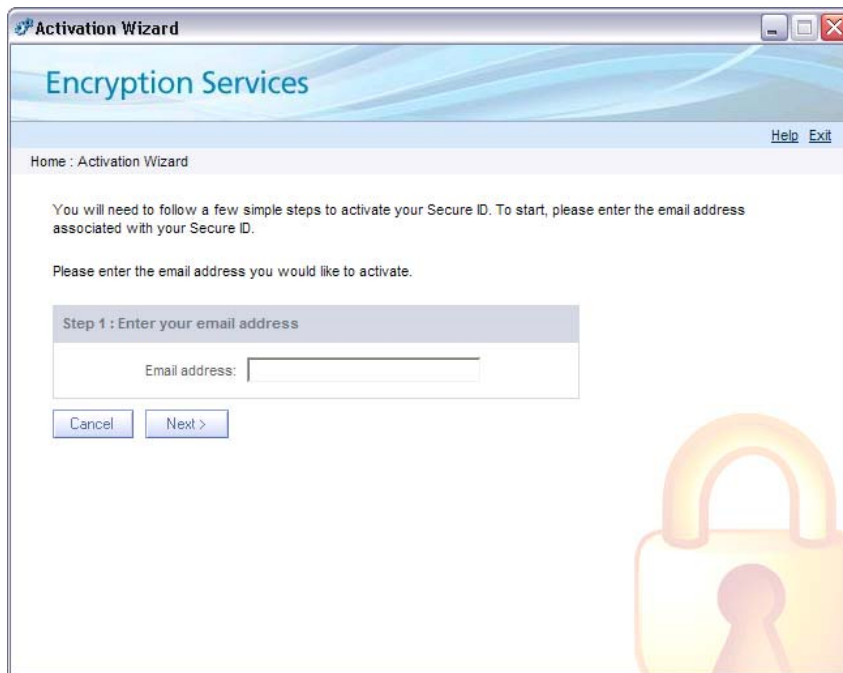
13 To complete the installation, click **Finish**.

Activating Your Secure ID

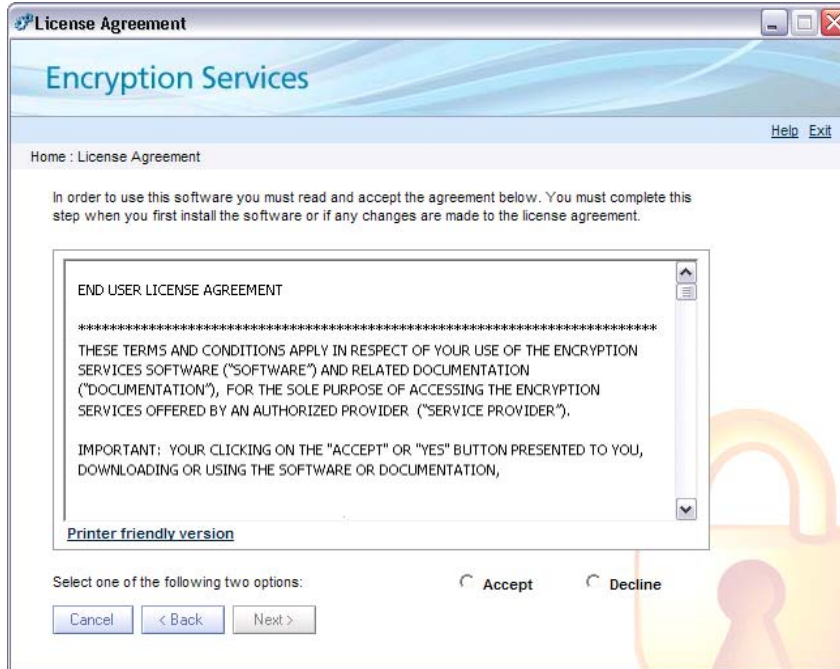
Activation for New Users

If you have never previously activated your Encrypted Mail, you will need to complete the following:

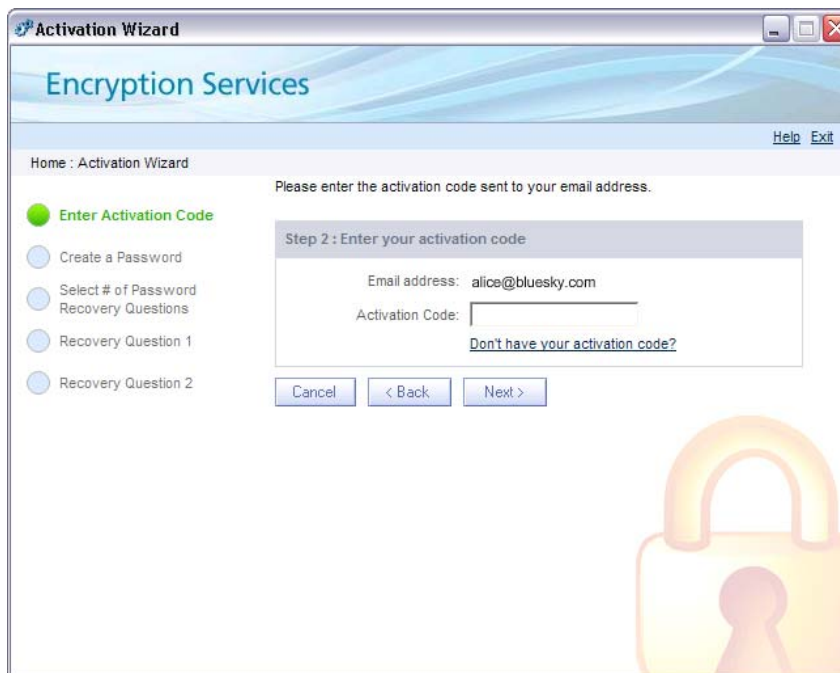
- 1 Open the Activation Wizard:
 - If the **Activate my software now** checkbox was selected after installing Encrypted Mail, the Activation Wizard will open automatically.
 - If you did not select the **Activate my software now** checkbox, you can continue the setup by opening Outlook.



- 2 Enter your email address as it appears on your 'Getting Started' email and then click **Next**. The license agreement appears.



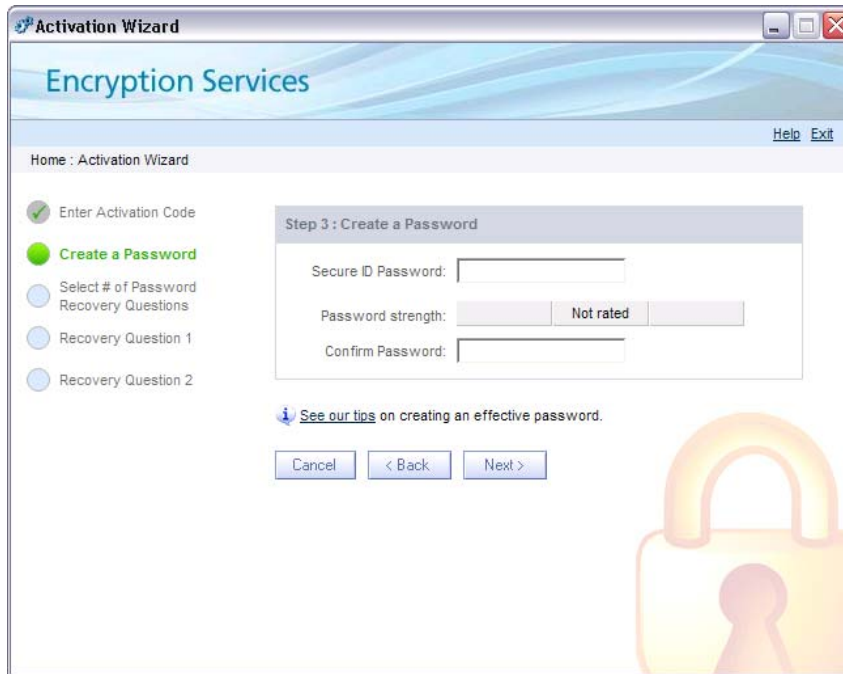
- 3 Read the license agreement. If you accept the terms, select **Accept** and then click **Next**. The Enter Activation Code window appears.



- 4 Enter your Activation Code exactly as it appears on your 'Getting Started' email.

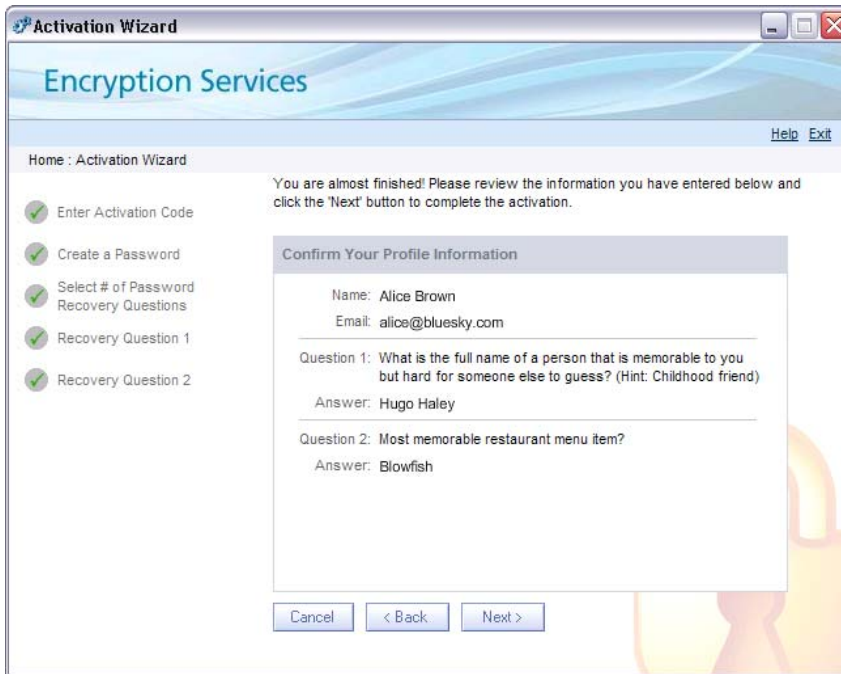
If you are prompted for your Secure ID password at this step instead of your activation code, it means you have previously activated your software. To continue activating Encrypted Mail, refer to Step 4 of [Activation for Existing Users, page 17](#).

- 5 Click **Next**. The Create a Password page appears.



- 6 Enter a Secure ID password and then re-enter the password to confirm. The *Password strength* bar will display the complexity of your password (weak, medium, strong). For tips on creating a secure password, see [Tips on Creating an Effective Password, page 41](#).
- 7 Click **Next**.
- 8 You must now create a series of password recovery question(s) and answer(s). You will be prompted to select a question and then enter the answer to these questions in the event you forget your password and need to reset it. Select questions that you will easily be able to answer, but hard for others to guess.

- 9 Click **Next**. The Confirm Your Profile Information page appears.



- 10 Review the information you have entered.

To continue, click **Finish**. To edit any information before continuing, click **Back**.

Once the activation process is complete, you will receive a confirmation screen.



- 11 Click **Finish**. The I Want To... page appears with links to a tutorial and information about your Secure ID.



Activation for Existing Users

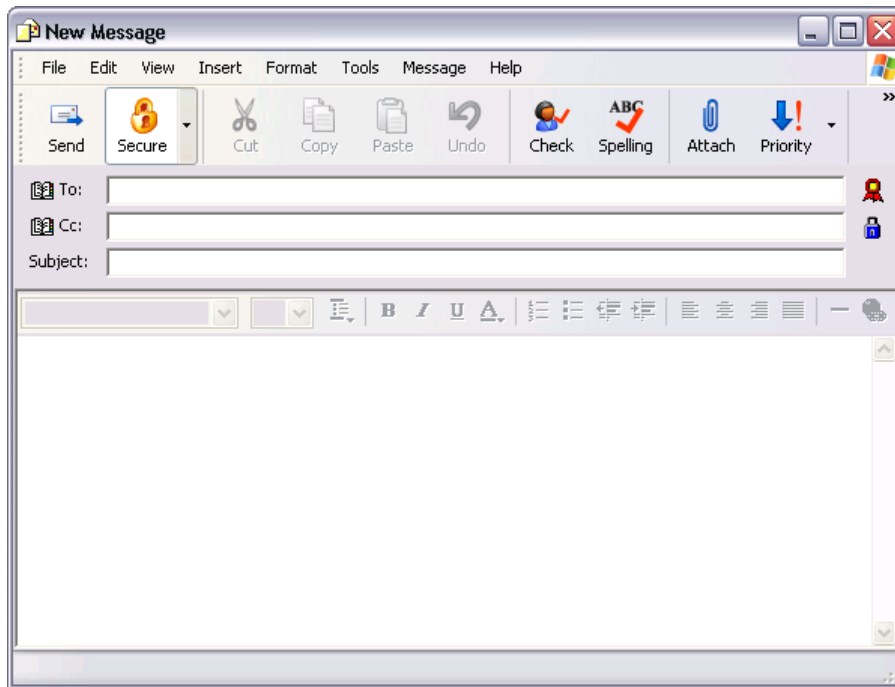
If you have previously installed and activated Encrypted Mail but would like to re-install Encrypted Mail or install/activate it on another computer, complete the following steps:

- 1 Open the Activation Wizard.
- 1 Enter your email address exactly as it appears on your 'Getting Started' email.
- 2 Click **Next**.
- 3 Enter the Secure ID password associated with this email address.
- 4 Click **Next**. Once the activation process is complete, you will receive a confirmation screen.
- 5 Click **Finish**.

Validating Your Installation

Once you've successfully installed and activated Encrypted Mail, you can validate the Encrypted Mail Outlook Express/Windows Mail installation by checking the following:

- Click the **Start** button and then select *All Programs*. An encrypted mail folder appears in the list of programs.
- From the Outlook Express/Windows Mail *File* menu, click **Tools**. An encrypted mail option appears.
- From Outlook Express/Windows Mail, click **Create Mail**. A *Secure* button appears on the *Standard* toolbar.



Sending a Test Message

To validate that Encrypted Mail is installed correctly, send a test encrypted message to yourself and open it by completing the following steps:

- 1 From Outlook Express/Windows Mail, compose a short message with "Test" as the *Subject*.
- 2 Address the message to yourself.
Note: Ensure you use the email address associated with Encrypted Mail.
- 3 Click **Secure**.
- 4 Click **Send**. The password prompt appears.
- 5 Enter your Secure ID password.
- 6 When the test message appears in your Inbox, open the message. The password prompt appears.
- 7 Enter your Secure ID password.
- 8 Click **OK**. The test message is decrypted and the contents appear.

Using Encrypted Mail

This section of the guide covers the following topics:

- Sending an Encrypted Message
- Sending a Digitally Signed Message
- Viewing an encrypted message
- Encrypted Mail Tools & Settings
- ID & Password Tools
- Adding a Trusted Contact
- Uninstalling Encrypted Mail

Sending an Encrypted Message

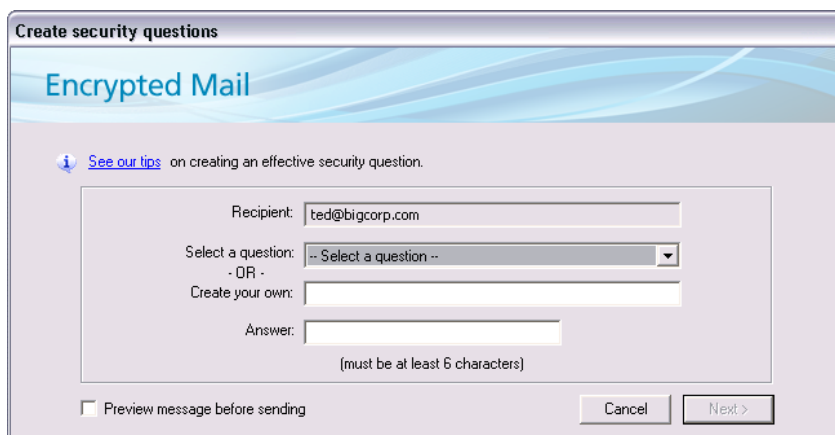
Encrypted Mail allows you to send an encrypted message to any recipient, including those that are not Encrypted Mail subscribers.

To send an encrypted message:

- 1 Compose a new message and attach any files.
- 2 Click **Secure**.
- 3 Click **Send**.

Tip: If you forget to secure a message, you will be prompted by default with a reminder prompt. For more information on the reminder prompt, see [Setting the Encrypted Mail Reminder Prompt, page 24](#).

- 4 At this point, Encrypted Mail will automatically check to see if your recipient(s) subscribe to the Encrypted Mail:
 - If all of your recipients are Encrypted Mail subscribers, the password prompt will appear. Continue to step 5.
 - If one or more of your recipients are **not** Encrypted Mail subscribers, you will be prompted to create a security question and answer.




The screenshot shows a dialog box titled "Create security questions" with the "Encrypted Mail" logo. It contains a link to "See our tips" and a form with the following fields: "Recipient:" with the value "ted@bigcorp.com", "Select a question:" with a dropdown menu showing "-- Select a question --", "OR", "Create your own:" with an empty text box, and "Answer:" with an empty text box and a note "(must be at least 6 characters)". At the bottom, there is a checkbox for "Preview message before sending", a "Cancel" button, and a "Next >" button.

The security question is used to ensure the identity of the recipient and protect the message from being intercepted by someone other than the intended recipient. Before the recipient can read the message, they will be prompted to answer your security question. If the question can not be answered correctly, the recipient will not be able to open the message.

Once you have created a security question and answer, click **Next**. The password prompt appears.

- 5 Enter your Secure ID password.



The screenshot shows a dialog box titled "Enter Your Password" with the "Encrypted Mail" logo. It contains the following fields: "Email address:" with the value "alice@bluesky.com" and "Password:" with an empty text box. At the bottom, there is a link for "Forgot your password?", an "OK" button, and a "Cancel" button.

- 6 Click **OK**. The message is encrypted (or scrambled) and digitally signed.

Tips on Sending Encrypted Messages

Encrypted Mail and File Sizes

As a general rule, when an encrypted message is encrypted the size of the message will increase by a factor of 2.5. The final size of the encrypted message is largely dependant on the size and file format of any attachments.

Size of original message with attachment(s) in MB	Approximate size of encrypted & signed message in MB
1	2.5
2	5
3	7
5	12.5

The maximum allowable email size depends on the policy set by your company or email service provider. For large files you may want to consider using a compression utility such as WinZip and/or sending the attachments in batches.

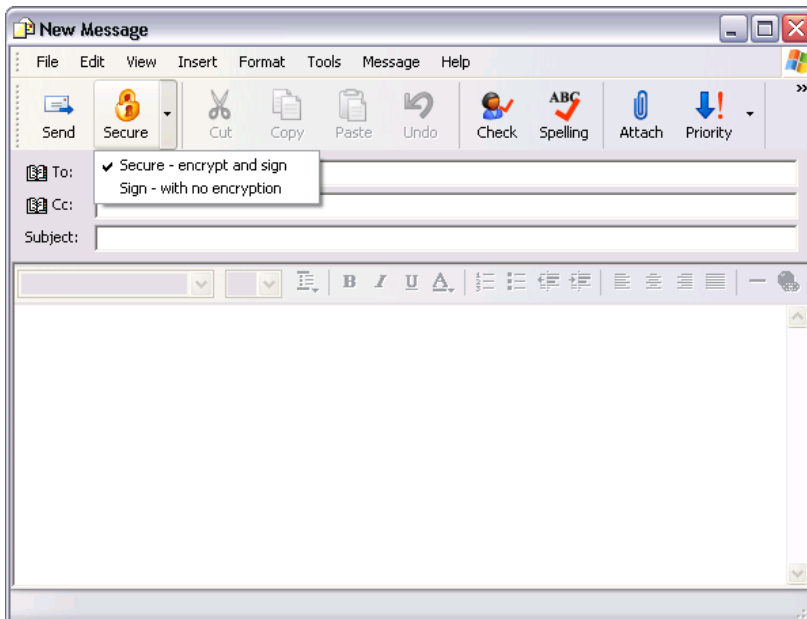
Sending a Digitally Signed Message

Another feature of Encrypted Mail is the ability to just digitally sign a message before sending it to the recipient. When a message is digitally signed, the recipient can be positive that the message is from the sender and that it was not modified in any way.

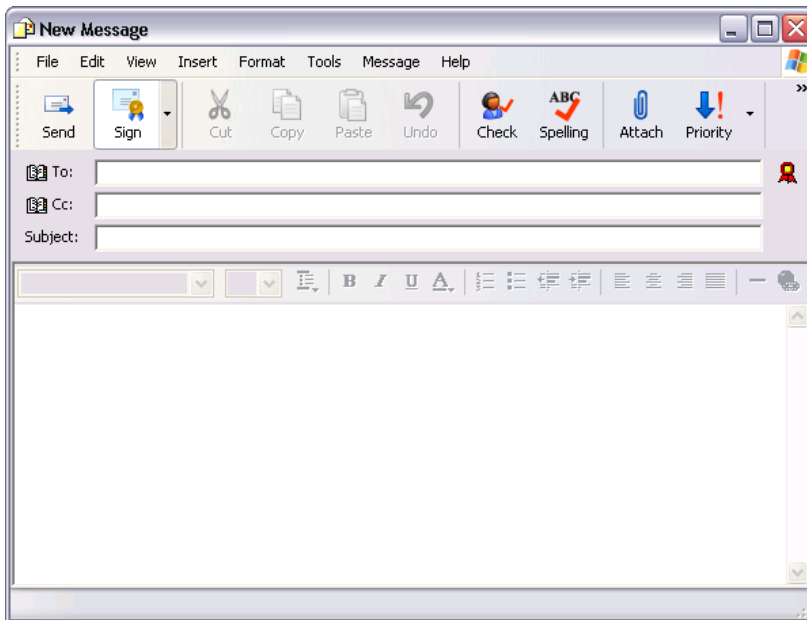
Important: A digitally signed message is not an encrypted message. If you require a digitally signed and encrypted message, see [Sending an Encrypted Message, page 20](#).

To send an encrypted message, follow these steps:

- 1 Compose a new message and attach any files.
- 2 Click the downward arrow next to the Secure button.



- 3 Select **Sign – with no encryption**. The *Sign* icon appears on the toolbar.



- 4 Enter your Secure ID password.
- 5 Click **OK**. The message is digitally signed.

Multiple Email Accounts in Outlook Express/Windows Mail

If you have multiple email accounts configured in Outlook Express/Windows Mail, always ensure your *Send From* email address is the address associated with your Encrypted Mail ID.

- To select the *Send From* address in a new message window, click **From:** and then select the appropriate email address

Setting the Encrypted Mail Reminder Prompt

What is the Encrypted Mail Reminder Prompt?

Have you ever sent an email that mentions an attachment, and then forgot to attach the file? If so, you'll understand why the **Encrypted Mail Reminder** prompt can be helpful. It can be a little embarrassing to forget an attachment, but forgetting to secure a confidential email can be disastrous.

By default, the Encrypted Mail Reminder prompt is enabled, offering a safety net in the event you forget to secure your message. However, some users do not want to be prompted each time they send a message. The following describes how to disable and re-enable the reminder prompt.

Disabling the Encrypted Mail Reminder Prompt

To disable the Encrypted Mail Reminder prompt:

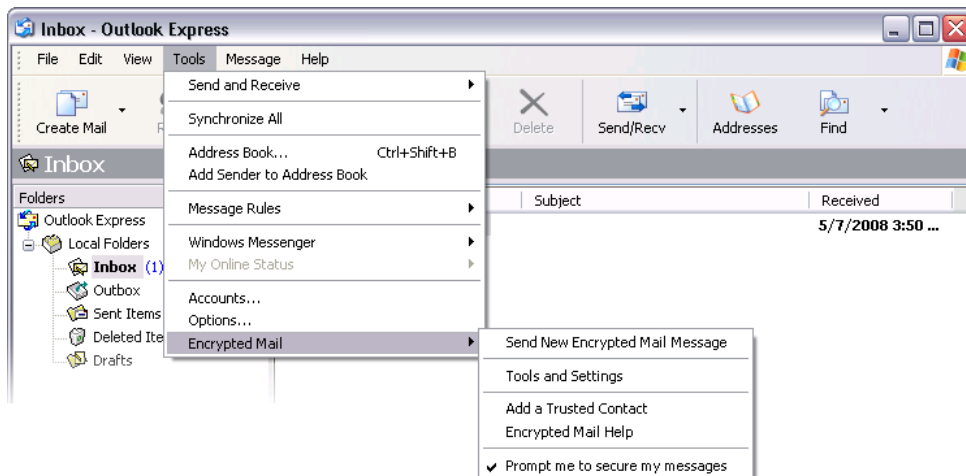
- When the prompt appears, select the *Please don't prompt me again* checkbox. The prompt will no longer appear when you send a message



Enabling the Encrypted Mail Reminder Prompt

To re-enable the Encrypted Mail Reminder Prompt:

- From the Outlook Express/Windows Mail main window, click **Tools** and then select *Encrypted Mail > Prompt me everytime I Send Email*. The prompt will appear the next time you send a message.



Viewing an encrypted message

There are two ways you can view an encrypted message:

- Subscribers of the service receive encrypted messages directly to their email inbox and simply enter their Secure ID password to open the message.
- Non-subscribers receive a notification message which directs them to the Message Pickup Center to retrieve their encrypted message. They are prompted to answer a security question set by the message sender in order to decrypt and open the message.

Viewing an Encrypted Message as a Subscriber

Encrypted messages appear in your Outlook Express/Windows Mail Inbox with a lock icon. Messages will remain encrypted in your Inbox, even if you leave your computer unattended.

Depending on your version of Microsoft Outlook Express/Windows Mail and how you have configured your Encrypted Mail settings, you will see one of the following lock icons:

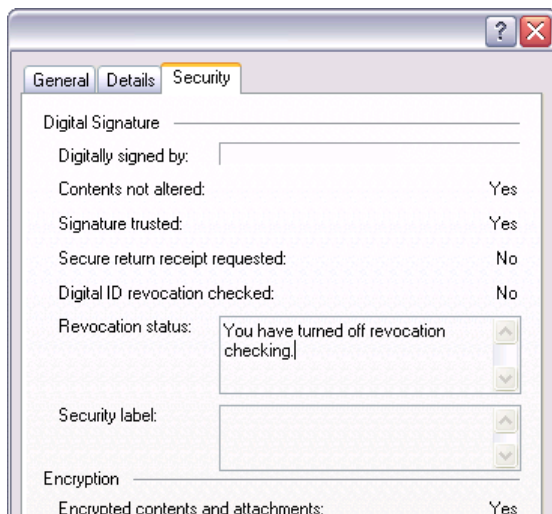
To view the encrypted message:

- 1 Double-click on the encrypted message. The password prompt appears
- 2 Enter your password.
- 3 Click **OK**. If you have successfully entered your password, the message appears.

Verifying the Sender

To verify that the message has not been altered:

- At the top right of the encrypted message, click the blue lock or red ribbon.



Viewing an encrypted message as a Non-subscriber

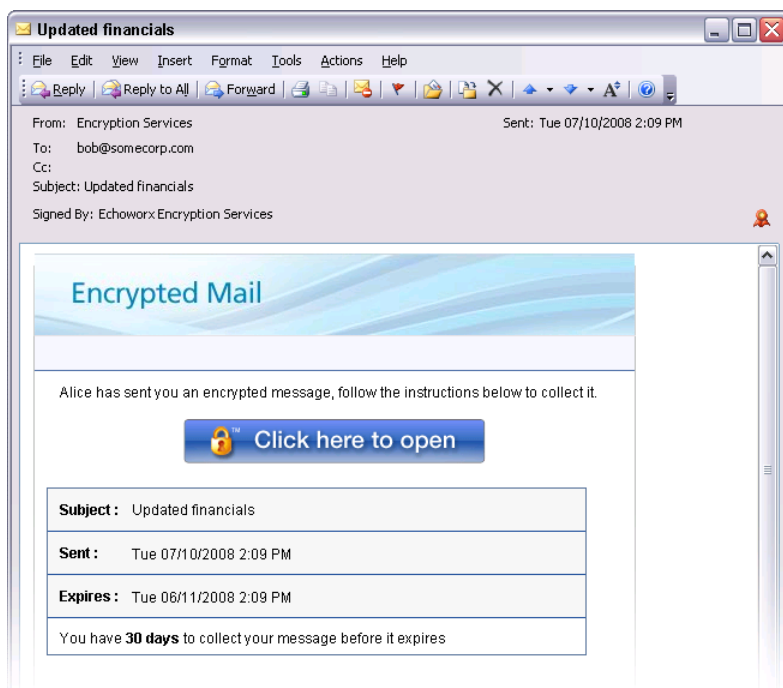
Encrypted messages sent to non-subscribers are encrypted, digitally-signed and then sent to the Message Pickup Center to be stored securely until the recipient retrieves the message.

The recipient receives an Encrypted Mail notification in their inbox which contains some basic information about the message and a link to open it.

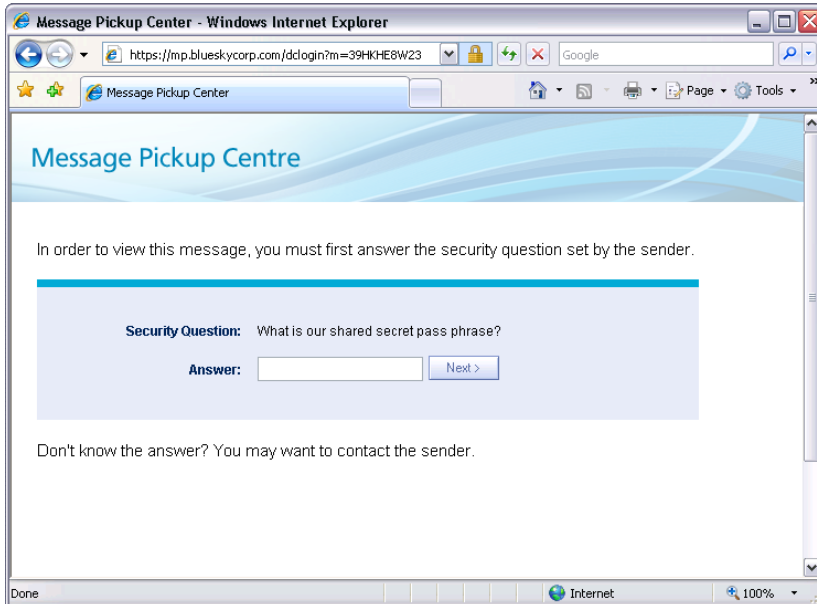
Note: Users who do not have email software capable of displaying HTML formatted messages will see a plain text version of the notification.

To view the encrypted message:

- 1 Open the notification message.



- 2 Click **Open message**. The Message Pickup Center window appears with the Security Question.

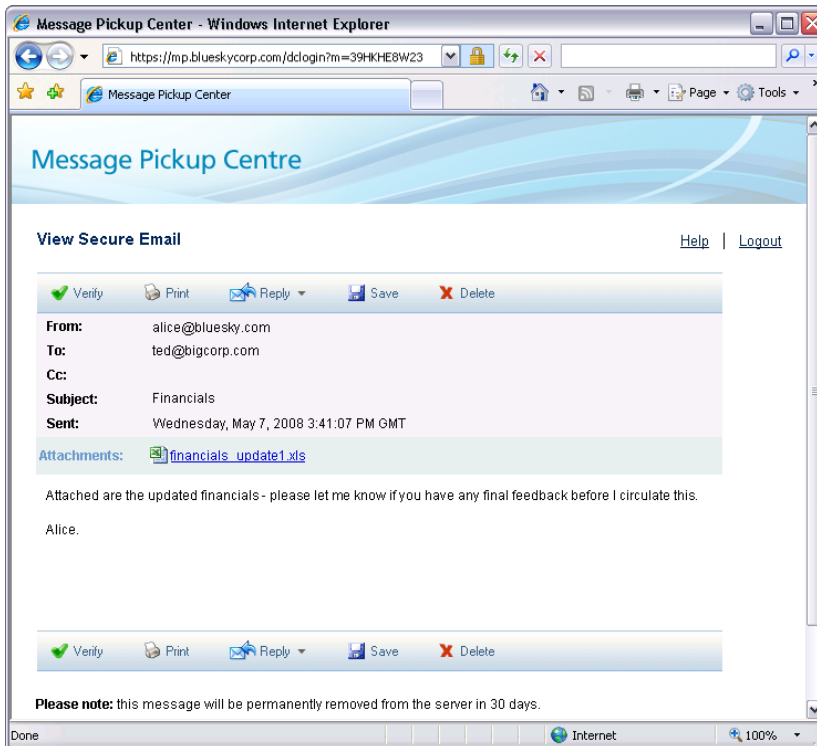


- 3 Enter the answer to the Security Question.

Note: You have three attempts to answer the security question. After three incorrect answers, the message is locked for a period of three hours before you can try again.

- 4 Click **Continue**. If you successfully answered the security question, the message is decrypted and appears.

Once the message is open, you can verify the integrity of the message and the sender, print, delete or save it (and any attachments).



Encrypted Mail Tools & Settings

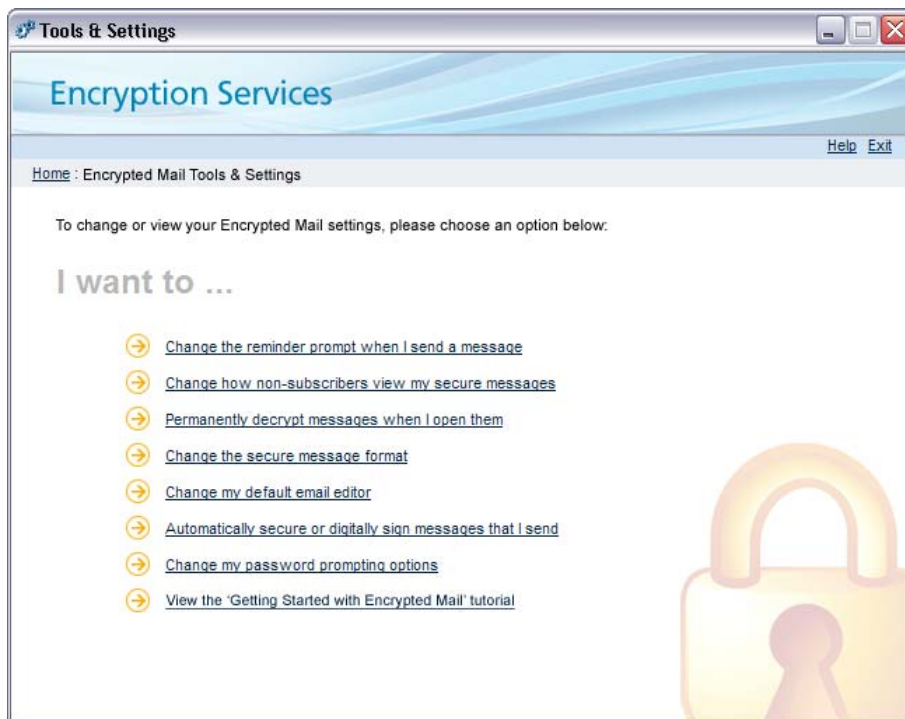
The Encrypted Mail Tools & Settings allows you to edit your Encrypted Mail settings, including:

- Configuring the Reminder Prompt
- Changing how non-subscribers view encrypted messages
- Permanently decrypting messages
- Choosing whether messages are automatically digitally signed/secured
- Configuring password prompting options

Viewing the Encrypted Mail Tools & Settings

To view the Encrypted Mail Tools & Settings:

- 1 Open Tools & Settings:
From the Outlook *File* menu, click **Encrypted Mail** and then select *Tools and Settings*; or, Click **Start** and then select *All Programs > Encrypted Mail > Tools & Settings*
- 2 Click **Encrypted Mail**. The Encrypted Mail Tools & Settings window appears.



Note: The following options are only available for Outlook users:

- **Change the encrypted message format**
- **Change my default email editor**

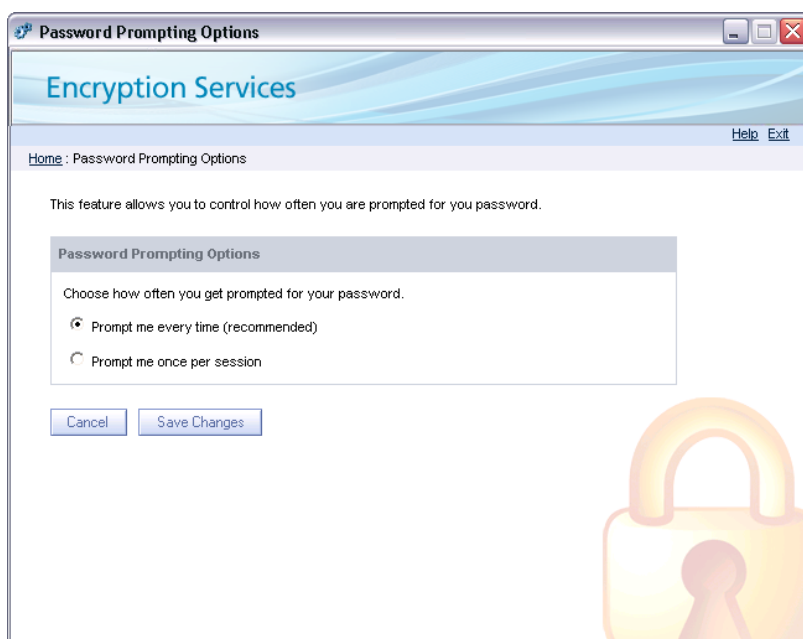
Changes to these options will not affect Outlook Express/Windows Mail.

Configuring Password Prompting Options

For convenience, you may want to change how often you are prompted to enter your Secure ID password. By default, Encrypted Mail will prompt you for your password each time you open an encrypted message.

To configure password prompting:

- 1 From the Encrypted Mail Tools & Settings tab, click **Change my password prompting options**.
- 2 Select a prompting option:
 - Select *Prompt me every time (recommended)* to be prompted for your password each time you open an encrypted message. ***This setting is strongly recommended.***
 - Select *Prompt me once per session* to be prompted for your password only when the first encrypted message is opened. Each additional time you will not be asked to re-enter your password until you reboot. By choosing this option, you are severely limiting the local security of Encrypted Mail.



- 3 Click **Save Changes**.

If you selected *Prompt me once per session*, a warning prompt appears. Read the message and the click **OK**.

The password prompt settings are updated.

ID & Password Tools

The ID & Password Tools tab allows you to edit your Secure ID settings and activate another Secure ID.

This section covers the following:

- Viewing the ID & Password Tools
- Backing Up / Exporting Your Secure ID
- Activating a New or Existing ID
- Recovering Your Secure ID
- Changing Your Secure ID Password
- Recovering a Forgotten Secure ID Password
- Configuring Password Prompting Options

Viewing the ID & Password Tools

To view the ID & Password Tools:

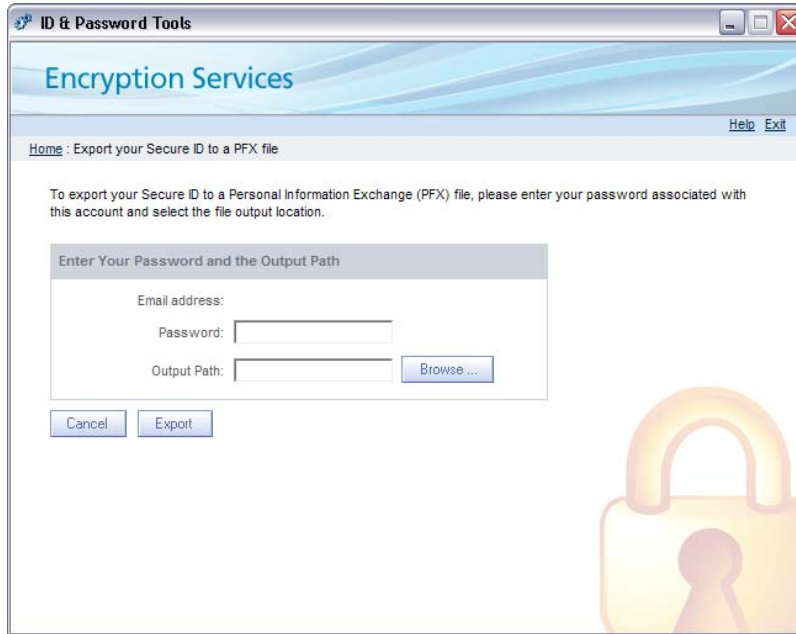
- 1 Open Encrypted Mail Tools & Settings.
- 2 Click the **ID & Password Tools** tab.



Backing Up / Exporting a Secure ID

To backup your Secure ID or make your private key exportable for use with a handheld device:

- 1 From the ID & Password Tools tab, click Backup / Export this ID.



- 2 In the *Password* text box, enter your password.
- 3 In the *Output Path* text box, enter the path to export the Secure ID. To select a path, click **Browse** and navigate to the appropriate location.
- 4 Click **Export**. The Secure ID is exported to the specified location and the *Mobile device enabled* status (under your ID profile) displays "YES".

Activating a Secure ID

If you add subsequent email addresses for Encrypted Mail, you can activate them within Tools and Settings.

- To activate another Secure ID, from the *ID & Password Tools* tab click **Activate a new or existing ID**. For the remaining steps, refer to [Activating Your Secure ID, page 13](#).

Recovering Your Secure ID

If your Secure ID is compromised in some way, customer support may instruct you to open the *ID & Password Tools* tab to recover it.

Note: In the event your Secure ID is removed or corrupted, the *Encrypted Mail Tools & Settings* will automatically prompt you for your email address and the associated Secure ID password in order to recover your Secure ID.

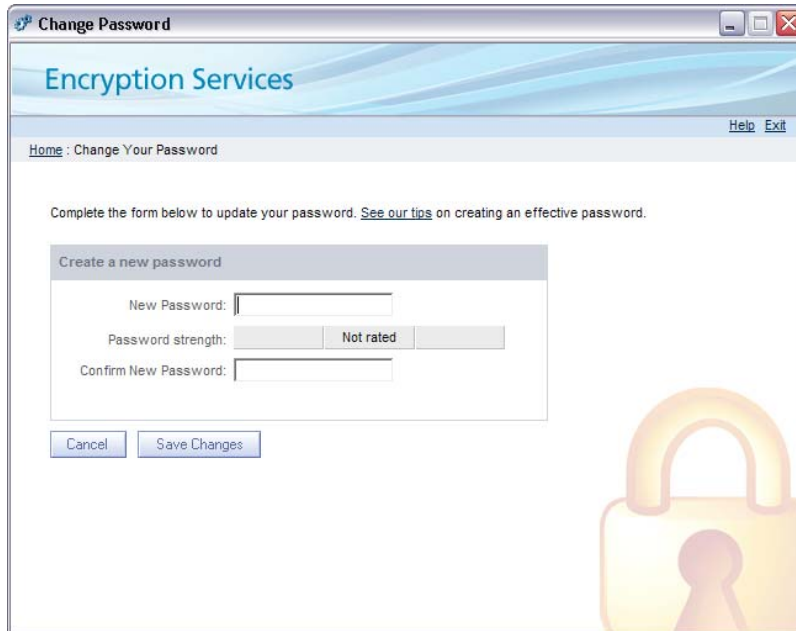
To recover your Secure ID:

- 1 From the *ID & Password Tools* tab, click **Add/Activate an ID**. The *Encrypted Mail Activation Wizard* appears.
- 2 Enter your Encrypted Mail email address.
- 3 Click **Next**. The password prompt appears.
- 4 Enter your Secure ID password.
- 5 Click **Next**. A confirmation message appears once the recovery is complete.
- 6 Click **Finish**.
- 7 Restart Microsoft Outlook Express/Windows Mail to complete the recovery

Changing Your Secure ID Password

To change your Secure ID password:

- 1 From the *ID & Password Tools* tab, click **Change my password**. The Change Password window appears.

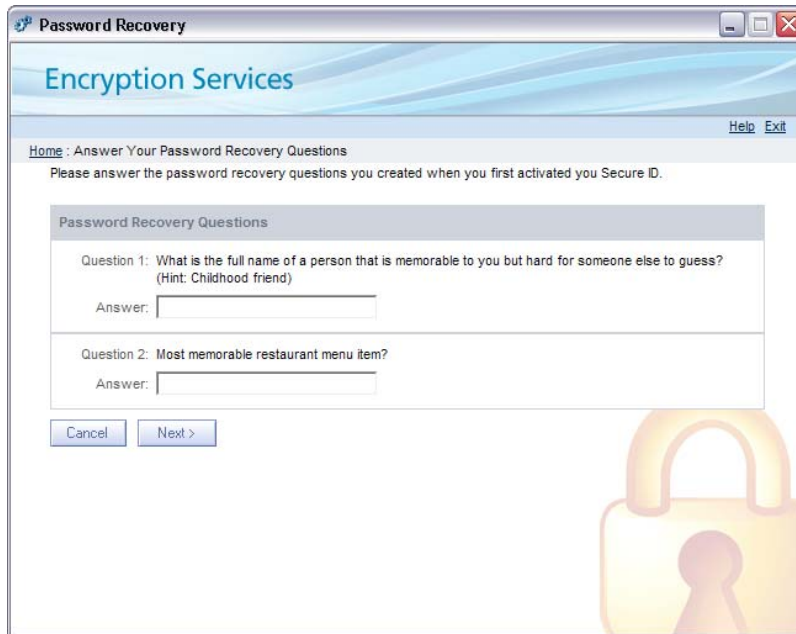


- 2 In the *Current Password* text box, enter your old password.
- 3 In the *New Password* text box, enter a new password.
- 4 In the *Confirm New Password* text box, enter the new password again.
- 5 Click **Save Changes**. Your Secure ID password is changed.

Recovering a Forgotten Secure ID Password

To recover a forgotten Secure ID password:

- 1 From the *ID & Password Tools* tab, click **I've forgotten my password and need to recover it.**



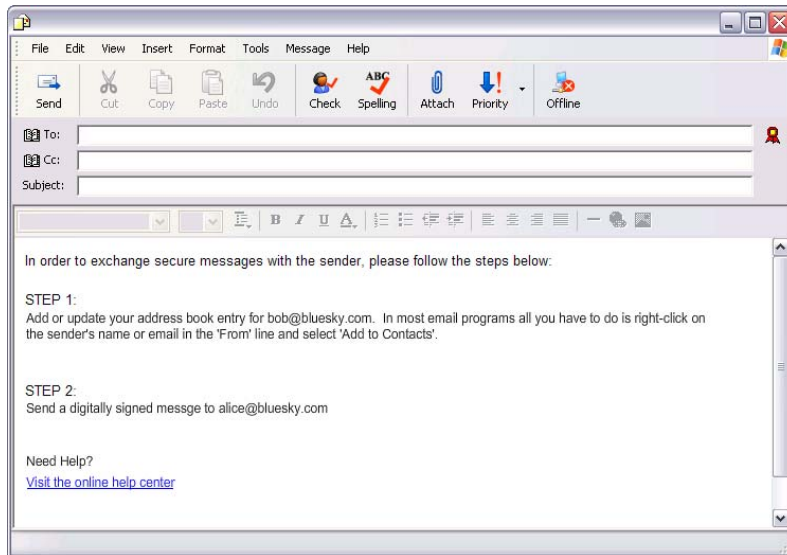
- 2 Enter the correct answers to the Password Recovery Questions.
- 3 Click **Next**.
- 4 In the *New Password* text box, enter a new password.
- 5 In the *Confirm New Password* text box, enter the new password again.
- 6 Click **Save Changes**. The new password has been created.

Adding a Trusted Contact

You can bypass the security question/answer step when sending a message to user of another compatible secure email system by adding the person as a trusted contact. This process is also called key exchange.

To send your public Secure ID (or public encryption key) and a request for someone else's key:

- 1 From the Outlook Express/Windows Mail *File* menu, click **Tools** and then select *Encrypted Mail > Add a Trusted Contact*. A new message window appears with a preformatted email message.



- 2 In the *To...* field, enter the email address of the person you want to add as a trusted contact.
- 3 Click **Send**.
- 4 Enter your Secure ID password.
- 5 Click **OK**. The message is digitally signed with a copy of your Encrypted Mail ID (public encryption key) and is sent to the recipient.

If the recipient responds to your request, the message appears in your Inbox with a red ribbon icon.

- 6 When the message is open, right-click on the sender's display name/email address (in the *From* line) and select *Add to Address Book*. The recipient's public encryption key is added to your local Outlook Express/Windows Mail Address Book.

Uninstalling Encrypted Mail

Note: When you uninstall Encrypted Mail, you will still be able to access your encrypted messages in Outlook Express/Windows Mail using your Secure ID password.

Uninstalling Encrypted Mail

To uninstall Encrypted Mail only:

- 1** Click Start and then select *Control Panel > Add or Remove Programs*.
- 2** Select *Encrypted Mail*.
- 3** Click **Remove**. A confirmation prompt appears.
- 4** Click **Yes**.
- 5** Once the installation is complete, a prompt appears. Select either:
 - Yes, I want to restart my computer now.
 - No, I will restart my computer later.
- 6** Click **Finish**. Encrypted Mail is uninstalled from your computer.

Support Information

This section of the guide covers the following topics:

- Frequently Asked Questions
- Tips on Creating an Effective Password
- Known Issues
- Error Messages
- Contact Information

Frequently Asked Questions

About Encrypted Mail

How much does Encrypted Mail cost?

Pricing is set by the carrier. Generally the service is offered as a Value Added Service with a fixed monthly recurring fee.

Can I use my existing email address?

Yes. You can sign up for Encrypted Mail using any email account as long as you are using a supported desktop email client to send and receive messages.

Who can I send Encrypted Mail email messages to?

Encrypted Mail subscribers can send encrypted messages to anyone. Your recipients do not need to be subscribers in order to receive encrypted messages.

Is Encrypted Mail standards-based?

Yes. Encrypted Mail has been developed using trusted industry standards - public key infrastructure (PKI), digital certificates (X.509), and Secure / Multipurpose Internet Mail Extensions (S/MIME).

Signing up for Encrypted Mail

Can I secure my Hotmail, Gmail, Yahoo, or other webmail account?

Yes. However, you must use a supported desktop email client (e.g., Outlook, Outlook Express/Windows Mail) to access the email account. This is generally done by configuring the email account as a POP account within the supported mail client.

How can I determine if I meet the minimum system requirements for Encrypted Mail?

Visit the Encrypted Mail Self-Care website and download the System Check Wizard. This application will determine if your computer meets the minimum system requirements to install and use Encrypted Mail.

Why are some Encrypted Mail Tools & Settings options greyed-out?

Your Encrypted Mail provider may restrict which options you can customize on the Encrypted Mail Tools & Settings window. If an option is restricted, it will appear greyed-out. For more information, please contact your Encrypted Mail provider.

Downloading and Installing

Why am I unable to download the Encrypted Mail Installer or System Check Wizard?

It is likely that you are behind a corporate firewall that is blocking your ability to download executable (EXE) files. The Encrypted Mail Installer and System Check Wizard are available as a ZIP files from their respective download pages. You may want to involve your help desk if you are having difficulties downloading either application.

How big is the Encrypted Mail Installer file?

The Encrypted Mail Installer file is approximately six (6) megabytes in size.

Can I install Encrypted Mail on multiple computers?

Yes. There is no limit to the number of computers you can run the Encrypted Mail Installer on. The first time you activate your email account you will be prompted for your activation code. On subsequent installations you will be challenged to supply your Secure ID password instead of the activation code.

How do I reinstall Encrypted Mail on my new PC?

As an existing Encrypted Mail subscriber, all you need to do is download and run the Encrypted Mail Installer. Once you have completed the install, the system will recognize that you are an existing subscriber, and you will be challenged to supply your Secure ID password. Upon correctly entering the password, your Encrypted Mail ID information will be downloaded and stored on your new PC. You are now ready to use Encrypted Mail.

I've lost my activation code, now what?

Your activation code is sent via email to the email account that was registered for use with Encrypted Mail. If you no longer have this email message, you (or the account manager for your company) will need to login to the Encrypted Mail Self-Care web site to resend the activation code.

I didn't receive an activation code, now what?

If you are using anti-spam software, it is possible that the email containing your activation code may have been flagged as spam. Please check the junk or spam folder for your activation code.

Sending Encrypted Mail

Who can I send Encrypted Mail email messages to?

Encrypted Mail subscribers can send encrypted messages to anyone. Your recipients do not need to be subscribers in order to receive encrypted messages.

Is there a file size limit when sending Encrypted Mail?

The same file size limits apply to encrypted messages as they do to regular message. Please see your Acceptable Use Policy for details on size limits.

Note: When a message is encrypted (or scrambled) using Encrypted Mail, the message size could double or triple depending on the content and attachment type(s).

Why am I only prompted to enter my Secure ID password to send an encrypted message, other times I also have to assign a security question and answer for my recipients?

With Encrypted Mail you can send an encrypted message directly to other subscribers of the service, or, you can send to non-subscribers. When you send to another subscriber - you are only prompted for a password, and the email goes directly from your PC to their inbox. When sending to a non-subscriber, you must attach a security question and answer to your message that the non-subscriber must answer correctly when they go to retrieve the secure email message.

Receiving Encrypted Mail

Why do some of my recipients receive my secure email messages directly into their inbox, while others have to go to a website to retrieve it?

Recipients that receive the messages directly are also subscribers to the Encrypted Mail service. For those recipients that are not subscribers of Encrypted Mail, they will be directed to a website to retrieve the email message.

I keep sending an encrypted mail message to a friend (a non-subscriber), who says he never receives the notification message - what's the problem?

There are two possibilities. It is very likely that the recipient is using an anti-spam package that is falsely flagging the message as spam, or, the recipient is using a white-list filter and does not recognize who is actually sending the notification message. Have the recipient check their Junk or Spam folder being used by their anti-spam software to see if the notification message was flagged. If the message was blocked because of a white-list restriction, they should add the sender of the notification message to their white list. This name is not the sender of the original email, but rather the email address of the Encrypted Mail service that sends the notification message.

How do I know whether my recipients retrieved my Encrypted Mail messages from the Message Pickup Center?

If you send an Encrypted Mail message to someone and it is not retrieved from the Message Pickup Center, you will receive an email notification message at the end of the message holding period stating that a specific person did not retrieve the message. In this case you should contact the recipient and let them know that you are resending the message, and that they should pick it up as soon as possible. If they are not receiving the Encrypted Mail notification message, please see the FAQ entitled "I keep sending an encrypted mail message to a friend (a non-subscriber), who says he never receives the notification message - what's the problem?" for more information.

Is the message stored at the Message Pickup Center secure?

Yes. The message is encrypted in a similar fashion as sending to another Encrypted Mail subscriber. The recipient of the message must correctly answer the secret question in order open the encrypted message.

How long will the message be retained on the Message Pickup Center in order for me to retrieve it?

This is a configurable parameter that is set by the service provider. When you send a secure email message to a non-subscriber, the length of the message holding period is included in the Encrypted Mail notification message. The message must be picked up within this time period, otherwise it will be deleted.

If an Encrypted Mail message on the Message Pickup Center expires and is deleted, can it be recovered?

No. The only way to get a copy of the message after it has been deleted on the Message Pickup Center is to ask the original sender to resend the message.

I don't know the answer to the question that was assigned to the Encrypted Mail message I was notified to pickup. What now?

Contact the sender of the email message to find out what the answer is to the challenge question.

Can someone try to hack into the Encrypted Mail Message Pickup Center to retrieve my encrypted mail message?

No. Protection has been put in place to block automated attempts at guessing your password. After 3 unsuccessful attempts the message cannot be accessed for a defined period of time. This period of time is defined by the Service Provider.

Can I forward a message in the Message Pickup Center to another person?

Not directly. You can only 'Reply' to the sender or 'Reply All', however you can also add other recipients to this list if you wish. Be advised that the message reply (or forward) is NOT secure.

Tips on Creating an Effective Password

Your password is a critical piece of information when it comes to protecting your private information and digital identity. Here are a few tips to help you choose a strong password.

Good Passwords

Good passwords should be at least eight characters long.

They should include at least one character from each of the following three character groups:

Upper case alphabetic characters (A-Z),

Lower case alphabetic characters (a-z),

Numbers and symbols (0-9~`!@#\$\$%^&*()_-+={}[]\;:"<>',.~/)

Embed at least one number or symbol within the password rather than adding it to the beginning or end of an otherwise alphabetic string.

Bad Passwords

A bad password is one that is easily guessed by someone who knows you.

Examples of bad passwords include:

Your username

Your name or nickname

Names of anyone in your family

Your pet's name

Your birthday or family birthdays

Your phone number, social security number, or address

Do NOT make your password a dictionary word or common name with numbers and symbols merely substituting for similar looking alphabetic characters (e.g., "P@ssw0rd"). Most importantly, never share your password with anyone and do NOT write it down.

Remember to change your password regularly. This practice limits the amount of time that someone can use to guess your password and the amount of time that your password can be used if it is uncovered.

Strong Passwords Can Be Easy to Remember

A simple way to create a strong but easy-to-remember password is to take a phrase that means something to you and relate each word of the phrase to a corresponding letter, number or symbol. For example, the phrase "I am one happy student at Princeton University" could become the password Im1Hs@PU.

Known Issues

Several known issues have been identified during the course of testing the latest release. The list below includes the cause of the issue, a description of the problem and a recommended course of action if one exists.

Cause: Plaxo plug-in

Plaxo provides a plug-in to Outlook that interacts on several levels: email messages, Contacts and Task. This plug-in will attempt to alter message formats (place logos and contact information on the top of messages). In doing this, they will attempt to open encrypted messages and cause the triggering of password prompts. The prompts may appear several times and can be very annoying.

Solution: With Plaxo 2.0, users can now disable the Plaxo feature that attempts to change the email format (under Options, disable the email form display).

Cause: Anti-spam plug-ins

Anti-spam plug-ins (such as Norton, McAfee, etc.) will attempt to read email in order to apply anti-spam rules to the messages. When this occurs, the encrypted message will be opened - triggering a request for the password to decrypt the message. This is most evident on startup when the default message cursor is on an encrypted message.

Solution: From Encrypted Mail Tools & Settings, click **Encrypted message Format**. Select the *Use the Microsoft Format* checkbox and then click **Save Changes**.

Cause: Yahoo Toolbar

If you are using the Yahoo toolbar and have the popup blocker enabled, some options typically available within a decrypted message on the Message Pickup Center (verify, print etc) are disabled.

Solution: Temporarily disable the pop-up blocker when collecting messages at the Message Pickup Center.

Don't see your issue listed? You can email with your issue or questions directly!

Support will attempt to respond within 24 hours after being contacted.

Error Messages

This section describes the different error messages you may receive and what you should do if you receive one.

A request to service was denied

When you receive the A request to service was denied message it means your access to the service has been cancelled. In this situation, you can phone customer support to renew your subscription.

Services are currently not available

When you receive the Encrypted Mail services are currently not available message it means your client is unable to establish contact with the Encrypted Mail services. This could mean one of the following things:

The services are temporarily not available. Try again in a few minutes.

Your access to the service has been cancelled. In this situation, you can phone customer support to renew your subscription

If you receive this message when you open Outlook Express/Windows Mail, you do not have Internet access. Check your local connection.

Cannot establish connection to server

When you attempt to send an encrypted mail and receive the following message, it is a local problem. Check to make sure you still have a connection to the Internet. You can do this by simply opening your web browser.

Have a Comment, Question or Need Support?

If you have a comment, question or require technical support, please email info@echoworx.com or call 1-416-226-8628 anytime between 9:00 AM and 5:00 PM (EST) from Monday to Friday.

Appendix A: Email Security Concepts and Terminology

This appendix describes the following concepts and terminology:

- Information Security
- Privacy Versus Security
- Identity Management
- Cryptography
- PKI and Digital Certificates

Information Security

There is no such thing as absolute security; it is not a state, it is a process. Information security is all about risk management; it is about balancing the potential loss against the cost of security measures that mitigate the threats. The costs of an incident may include tangible losses in the form of equipment, information, money or time, or intangible losses such as reputation, which may be even more precious to an organization. Yet, such potential costs must be assessed with regard to the probability of occurrence.

There are various kinds of threats that an organization needs to consider, which may involve the unauthorized disclosure, destruction, alteration or fabrication of information, or the unauthorized use of services and resources. Attention is most often given to defending against adversarial sources such as competitors, criminals, hackers, malicious individuals (crackers) or disgruntled insiders (well-situated to do great harm). However, a holistic security regime should also address the unintended consequences of accidents or natural disasters.

For intentional acts, there are various modes of attack, that can be classified as being either passive, such as eavesdropping on communications, or active, such as tampering or fabricating transactions. Some attacks are technical, relying solely on the use of technology to achieve some objective but many (perhaps most) rely to some degree upon social engineering – the art of eliciting sensitive information or assistance from a person in a position to be helpful to the adversary. Some forms of social engineering are quite subtle, involving the psychological or sociological techniques of confidence games in which the target may be an unwitting participant, while at the other end of the spectrum are brute force techniques of coercion, such as bribery, blackmail or worse.

There is an ongoing 'arms race' between adversaries and security practitioners with a continual escalation in the application of techniques and technologies as security measures and countermeasures. Not all security threats can be foreseen or protected against. Moreover, for many the cost of defence may far outweigh the cost of remediation. Therefore a comprehensive approach to security should include measures and countermeasures for deterrence, defence and detection: those assets for which threats cannot be deterred should be defended; those threats which cannot be defended against should be detected and followed by appropriate remedial action (which may include strengthening security practices and litigation to recover damages).

The point of this introduction is not to educate the reader on the many fine points about information security but merely to convey the breadth and depth of the topic. In particular, it serves as preamble to the assertion that whilst cryptography is an important technology in this field, it does not assure security by itself. Encryption, digital signatures, certificates and a public key infrastructure all contribute to a strengthened security posture but there is much more to assuring security that needs to be considered by an organization.

Too often, one hears about someone with a false sense of security from the understanding that something is secure because it is encrypted, yet not realize that the key used to protect that information is easily obtained by anyone able to read the yellow sticky note attached to the workstation! Security is a complex matter and no technology will solve all its problems.

Basic principles of information security

The basic principles of information security are as follows.

Identification and Authentication

User authentication is a process or mechanism that assures that the identity (or unique persona, in the case of pseudonymous systems) of a subject (person, program, system, etc.) has been satisfactorily verified;

Message authentication is a process or mechanism that assures that the identity of the sender of a message has been satisfactorily verified.

Confidentiality

Confidentiality is a property of sensitive information that satisfactorily assures it has not been disclosed to unauthorized parties.

Integrity

Integrity is a property of sensitive information that satisfactorily assures that it has not been altered or deleted by unauthorized parties.

Authorization

Authorization is a process that satisfactorily assures only duly designated or approved parties are granted permission to use or access sensitive information services or resources;

Access control

Access controls are mechanisms that satisfactorily assure that only duly authorized parties are permitted to use or access sensitive information services or resources.

Non-repudiation

Non-repudiation is a property of a security mechanism that satisfactorily assures that the authenticated subject(s) can be irrevocably and provably bound as a party to an action, transaction or communication, as a countermeasure against denial thereof (i.e., repudiation).

Privacy Versus Security

Confidentiality is an important aspect of both security and privacy, yet just as there is more to security, there is also more to privacy than keeping secrets – it is about ownership and control of personal information, its correctness and authorized use and/or disclosure to others for specified purposes. Privacy has to do with policies and their enforcement with respect to information assets that transcends the realm of information security, upon which it is dependent, although insufficient in itself. Secure email can certainly be used as a tool in protecting the communication of sensitive personal information but it is not a total solution to the full spectrum of issues concerning privacy.

Identity Management

Much of information security is dependent upon knowing the identity of entities of various kinds, whether a user, a program, a host machine, etc. Identity management is all about managing the identification, authentication and authorization attributes for entities within a system. In the following sections we shall see that a public key infrastructure (PKI) provides a means of identity management. An even simpler example is the password database on a traditional time-sharing host system.

For the purposes of simplifying the management and authorization of entities with various roles and privileges, we define the following terms used throughout this document:

- Realms
- Domains
- Subscribers
- Agents
- Servers

Realms

A realm is a collection of services and resources (e.g., hosts, databases, etc.) operated by authority under a common set of security policies and practices, which may be divided into one or more segments (each serving one or more application domains) plus any realm services and resources.

Domains

An application domain is collection of subscribers (end-user principals) subject to common end-user entitlements. Each end-user principal is a subject of exactly one domain for each application (i.e., having the same application identity). Multiple applications may share a common domain space (i.e., common credentials) with services and resources hosted in one or more realms, or applications may have separate domain spaces.

Subscribers

A subscriber is an end-user principal enrolled and entitled to use an application. Domains are comprised of users who are subscribers. Each subscriber has one or more public/private cryptographic key-pairs and associated digital certificates for use with the application. Subscriber certificates are issued under the auspices of a domain authority.

Agents

An agent is a privileged end-entity (person or software program) providing a realm- or domain-wide service or support role, such as a manager, operator or software service daemon. Agents may be issued certificates under the auspices of a realm or domain authority (although not the same issuer as for subscribers).

Servers

A server is an application container or service access point identified by a network host address and port number for communications with other end-entities. Application infrastructure servers are issued certificates under the auspices of a realm authority.

Cryptography

Cryptography is the process of communicating in or deciphering secret writings or ciphers. Encryption is the process whereby a plain or clear-text message is transformed into a cipher-text and decryption is the reverse process that yields the original message.

The following terms are used in cryptography.

Digital signatures

Some cryptographically produced information that attests to the authenticity of a document or transaction, such that it can be verifiably bound only to its originator.

Public Key Infrastructure (PKI)

Consists of the products, technologies, protocols, policies and authorities for the management and distribution of public-keys and digital certificates amongst parties within a specific application trust domain.

Note: For more information, refer to the section on PKI and digital certificates below.

Encryption

A cipher algorithm is usually a mathematical process for transforming a message from plaintext or clear-text to cipher-text or vice-versa. Such a process typically requires another secret piece of information, called a key, to effect this transformation. A cipher algorithm for which both parties, the sender and the receiver, use the same algorithm and same key is called a symmetric algorithm and the key is called a shared secret or symmetric key.

Without knowing the secret key, the symmetric cipher algorithm is useless. Indeed, it should be publicly known so it can be assured to be free from malicious code that might otherwise weaken the strength of the cipher, subtly rendering it vulnerable to some class of attack known by an adversary. It is important that well-known and proven algorithms are used in order to have assurance in the strength of the cipher.

Only parties sharing the secret key can communicate securely amongst each other; that is, only by using the same cipher algorithm with the shared secret key can either party encrypt a secret message intended for the other or can the recipient decrypt and read a secret message from the sender. No one else can read the original message. It is secure insofar as each party who has the secret key keeps it in confidence.

However, here we need to qualify secure, for whilst the confidentiality of the message is assured insofar as all the parties safeguard the secret key and the original message, there is no assurance as to the authenticity of the sender's identity. Any of the communicating parties could claim that any of the others is indeed the originator of the message. Even when just between two parties, there is an opportunity for one to fraudulently produce messages purported to be from the other.

Digital signatures

This problem was solved in the 1970s with the discovery of asymmetric methods of cryptography that lead to the concept of the digital signature. In asymmetric cryptography, differing but inversely related algorithms are used for encryption and decryption operations, each having its own key. As in the case of the symmetric cipher algorithms, the asymmetric algorithms should also be publicly known and trusted.

The associated pair of keys is called a key-pair; one must be kept secret, the private key, and the other may be disclosed to anyone, the public key. Any message encrypted with the private key can be decrypted with the public key and vice-versa.

This property means that any party who knows the public key can decrypt a message encrypted with the private key. At first glance, this might seem to undermine security because anyone can read the message, however given the message itself can be verified it allows anyone to verify the authenticity of the sender, since she is the only party in possession of the private key with which the message was encrypted.

The given assumption is easily met by using an immutable property related to the message; such as a one-way cryptographic hash function, such as MD5 or SHA-1, that essentially mathematically reduces the message to a unique numeric value. This same function can be computed by the recipient on the decrypted message and compared with the original. Consequently, we have the ability to produce a digital signature, unique to the sender.

The corollary to this property is that by a message encrypted with a party's public key can be decrypted only by that party. However, unlike symmetric algorithms, when a secret message needs to be communicated to several parties, it must be encrypted specifically for each party using that party's public-key.

In practice, however, due to the fact that asymmetric algorithms are far less efficient than symmetric algorithms, what is done is to first symmetrically encrypt the message using an arbitrary secret key is generated for specifically for this purpose; this secret key is asymmetrically encrypted with each recipient's public key; and then the cipher-text of the message and the cipher-text of the secret key is sent to the recipients. Upon receipt, the recipient can, using her own private key, decrypt the shared secret key and use it to decrypt the cipher-text message.

These methods can be put together in a couple of ways, depending upon whether the identity of the sender is to be secret or not.

- 1** A sender may first digitally sign a message, appending a cipher-text produced using their own private-key, and then encrypt the message and its digital signature for a number of recipients, and send it. The recipients must, in turn, decrypt the message using their own private keys, before the digital signature of the sender can be verified; or
- 2** A sender may first encrypt the message for a number of recipients and then digitally sign the cipher-text message, appending a digital signature produced using their own private-key, and send it. The recipients may verify the digital signature of the sender before decrypting the cipher-text message using their private keys.

PKI and Digital Certificates

As we have seen, public-key cryptography (PKC) is a very powerful tool for information security. Yet, it is only as secure as the keys can be trusted. This is where the concept of a public key infrastructure (PKI) is important. In general terms, a PKI is the particular collection of entities (individual persons, machines or services – including certification authorities, certified subjects and relying-parties), policies and technologies that define the scope of a trust domain in which public-keys are used.

Let's step back and consider why a PKI is needed: say Alice and Bob want to exchange secret messages; they would need to first exchange their public-keys. Now, consider that Eve was able to intercept that exchange and substitute her own public-key in place of Alice's; this would allow her to masquerade as Alice insofar as Bob is concerned – i.e., Eve and Bob could exchange messages, all the while with Bob believing that he was communicating with Alice. This is the problem that digital certificates are intended to solve.

A digital certificate is a special type of document that attests to the validity of the logical association or binding between a public-key and the identity of the subject key-owner (called a principal). This document is digitally signed by a trusted third-party called a certification authority (CA). A CA is responsible for verifying the identity of the owner of the public-key and assuring proof-of-possession (PoP) of the associated private-key before a certificate is issued.

Certification Authority (CA)

In the case of a public CA where there is no pre-existing relationship between the CA and the principal, the CA will demand proof of identity from the principal. Depending upon the class of service (i.e., the trustworthiness of the certificate requested), this identity information may be something as simple as an e-mail address or much more rigorous, requiring multiple national identity documents, an in-person interview and a background check performed by a security agency.

On the other hand, a CA operated by a commercial enterprise or ISP may leverage existing relationships with employees, customers and other affiliated parties so extensive verification processes need not encumber the issuance of certificates. Relying parties can be assured that the subject identity within an issued certificate has a business relationship with the organization.

The rules of engagement under which a certification authority operates is usually published in a document known as the Certification Practices Statement (CPS). This document and, more importantly, the definition and implementation of the practices themselves are the responsibility of the Certification Authority.

Registration Authority (RA)

There is often a separation between registration (enrollment and identity verification) and certification (the issuance of certificates for keys), so in addition to a CA, one may find a Registration Authority (RA) to whom this former role is delegated.

Key escrow

The term key escrow refers to the situation in which a principal's private key(s) are held in-trust by a trusted third-party and only released to another party upon fulfillment of certain authorization conditions.

Note: This key escrow model should only be applicable to cipher-keys; that is, keys used for message decryption – NOT signing keys, as to do so would violate the preconditions for non-repudiation: no other party should ever have access to the private key one uses for producing a digital signature.

There are two essential cases that need consideration:

- Lawful interception of communications for electronic surveillance; and
- Enterprise key management for asset protection (i.e., “corporate memory”).

In the first case, some jurisdictions require telecommunications carriers that provide secure messaging services to provide key escrow and recovery mechanisms to facilitate the lawful interception of communications (i.e., surveillance) by duly authorized law enforcement agents (e.g., pursuant to a court-ordered warrant). In the second case, an enterprise that assigns keys to be used by employees (or other authorized parties) may need to recover such keys in the event the employee is no longer available (e.g., died, fired, quit, etc.) to decrypt sensitive information necessary for the integrity of the collective corporate memory.

Appendix B: Privacy Legislation and Encrypted Mail

Privacy is Mandated by Law

Email travels from the sender to the receiver as a virtual postcard, and as email is stored and forwarded through the Internet, there is a real risk that someone other than the sender or the intended receiver can intercept and either read it or tamper with it. The content of email is now regularly finding its way into the news or into the hands of people who should not have it. The fact that large volumes of email can be collected, scanned, filtered, read and altered makes email an easier target for illegal interception than regular physical mail. Also, unlike regular mail, you would never know that your email has been intercepted and read or altered.

Encrypted Mail gives consumers and businesses alike the confidence that only the sender and the intended recipients are able to read email. Also, Encrypted Mail gives the recipients confidence that the sender is not pretending to be someone else, and that the message was not changed after the sender sent it. It's a value added service that gives subscribers the ability to send email to anyone with an email address, with the confidence that the email is securely encrypted and that only the persons to whom it is addressed can unlock it. With Encrypted Mail, everyone with an email address can send and receive encrypted digitally signed email, without knowing the details of how it's done.

Legislation

Email has become a dominant channel for personal and business communications. Everything from meeting requests to messages containing highly sensitive business or client information is sent by email. It is estimated that by 2006 there will be over 1.5 billion email boxes, operational worldwide. (Source IDC, 2003)

Everyone should take positive steps to protect this vital communications channel. Lawyers, financial advisors, accountants, educators, health care providers and other professional advisors have ethical and fiduciary duties to keep personal information about their clients' confidential information. Businesses need to be able to trust their email communications and reduce the risk of damage to their brand resulting from information obtained through intercepted email. Consumers are concerned about personal security, privacy, fraud and identity theft.

Governments have also enacted legislative measures to protect the privacy of personal information which either expressly or impliedly apply to personal information communicated electronically. Federal and state governments have enacted legislation that protects the privacy of personal information generally, as well as industry-specific legislation that protects confidential information from unauthorized disclosure and use.

Privacy legislation imposes a general obligation on businesses and government to protect the privacy and security of personal and private information. Some privacy legislation expressly requires that specific measures be taken to protect against unauthorized disclosure of electronically stored or communicated information. The test is whether "reasonable measures" have been considered and implemented to protect the privacy of personal information. There is no longer a reasonable expectation that email cannot be intercepted and read without authorization. With Encrypted Mail, encrypting email provides the necessary protection of this information and is a "reasonable measure" that should be used when communicating personal information via email.

Other industry-specific legislation protects the confidentiality and integrity of information relating to specific markets.

Health Insurance Portability and Accountability Act (HIPAA) is an example of legislation that protects personal information sent amongst health care professionals.

Sarbanes-Oxley Act (SOX) governs integrity of financial operations of publicly traded companies.

Gramm-Leach-Bliley Act (GLBA) requires that all financial institutions protect customer information.

California Security Breach Notification Act (CB 1386) requires disclosure when private personal information of a California resident has been compromised.

These are a few important examples of US Federal and State industry-specific legislation that directly or indirectly requires that information contained in email be protected against uncontrolled disclosure, and that requires companies to adopt sufficient measures to ensure integrity and authenticity of private information transmitted electronically.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes national standards to protect the privacy of personal health information by establishing standards that protect individually identifiable health information.

Health information is defined as any information, whether oral or recorded in any form, that relates to the past, present or future condition of an individual (HIPAA § 1171(4)). Individually identifiable health information is defined as health information that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

HIPAA is intended to ensure that health plans, doctors, hospitals and other health care providers take appropriate measures to control how personal health information such as patients' health records, test results, x-rays, and prescriptions, is used, disclosed and protected.

In order to take advantage of email communication for the efficient and timely transfer of patient information, health care practitioners must take reasonable measures to ensure that this information is protected from unauthorized access and disclosure.

Encrypted Mail provides a cost effective and easy-to-use mechanism for digitally signing and encrypting protected health information, and is therefore a "reasonable measure" for all entities that are subject to the legislation.

Encrypted Mail is a critical service that helps health care professionals to meet their legal obligation to keep personal health data of their patients private by providing an easy-to-use and safe mechanism for encrypting and digitally signing email messages.

Who is affected?

HIPAA states that security standards and requirements for the maintenance or electronic transmission of health information apply to the following persons:

Health Plans: generally including health, dental, vision and prescription drug insurers, HMOs, Medicare, Medicaid, and long-term care insurers;

Health Care Clearinghouses: for example, billing services, repricing companies or a community health management information systems; and

Health Care Providers who transmit any health information in electronic form in connection with a transaction for a "covered entity".

(HIPAA § 1172(a))

Examples of personal health information to which these standards apply include health claims or equivalent, encounter information, health claims attachments, enrollment and disenrollment in a health plan, eligibility for a health plan, health care payment and remittance advice, health plan premium payments, first report of injury, health claim status and referral certification and authorization (HIPAA § 1173(a)(2)).

Why Encrypt Email?

Encrypted email is an important communications channel for health care professionals. Each person listed above who maintains or transmits health information must maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of the information (HIPAA § 1173(d)(2)). These safeguards must also protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or disclosures of the information.

Under HIPAA, the Department of Health and Human Services publishes a Security Rule mandating that each covered entity develop policies, procedures and contingency plans for securing information. The HIPAA Security Rule does not expressly prohibit the use of email for sending electronic protected health information (PHI). The Security Rule allows for electronic PHI to be sent over an electronic open network as long as it is adequately protected.

The standards for:

- access control, (45 CFR § 164.312(a))
- integrity (45 CFR § 164.312(c)(1)), and
- transmission security (45 CFR § 164.312(e)(1))

require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against the unauthorized access to electronic PHI.

The standard for transmission security (§ 164.312(e)) also includes specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect electronic PHI as it is transmitted, select a solution, and document the decision.

Liability for Breach of HIPAA

In general, fines can be imposed by the Department of Health and Human Services on a person who does not comply with standards set forth under HIPAA (HIPAA § 1176(1)). The fine can be imposed each time an incident of non-compliance occurs, but will be capped at a maximum of \$25,000 per calendar year. The fine may not be imposed if the failure to comply with the standards was due to reasonable cause rather than to willful neglect and the issue resulting in a failure to comply is corrected within 30 days of when the person liable for the penalty knew or should have known about the lack of compliance (HIPAA § 1176(b)(3)).

In addition, a person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of \$50,000 and up to one-year imprisonment (HIPAA § 1177). The criminal penalties increase to \$100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to \$250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm (HIPAA § 1177).

Sarbanes-Oxley

The Sarbanes-Oxley Act of 2002 (SOX) introduced many legislative changes to the regulation of corporate governance and financial disclosure practice. The primary goal of SOX is to "protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws".

Encrypted Mail is an important service that helps companies in their compliance with SOX. Encrypted Mail provides companies that are subject to SOX with a simple yet highly secure means for ensuring that sensitive company information is transferred with the assurances that the information is not read without authorization; that information is not altered while traveling from the sender to the recipient; and that the email is digitally signed by the sender.

Who is affected?

Companies that must comply with SOX include U.S. public companies and foreign companies listing on U.S. stock exchanges or registering with the Securities and Exchange Commission (SEC). Many of the SOX provisions also apply to privately held companies with public debt.

Why Encrypt Email?

Quite simply, companies must ensure the effectiveness of the internal controls over financial reporting and compliance mandated by SOX. Since email has become one of the most pervasive communications channels, it is imperative that precautions are taken to ensure the integrity of sensitive financial information transmitted by email. Integrity of such information requires internal controls that ensure:

- Privacy. The content of email remains confidential and is not disclosed without authorization.
- Message Integrity. The content of email cannot be altered during transmission.
- Authenticity. The sender of email can be verified.

SOX § 404 regulates the enforcement of internal controls. Companies must establish and maintain internal controls over financial reporting, and must report on the internal controls and assess the effectiveness of these internal controls in their annual reports. The company's auditors must attest to these compliance reports.

"Internal controls over financial reporting" include processes designed to provide assurance as to the reliability of financial reporting and financial statements. Internal controls over financial reporting include policies and procedures that:

- pertain to the maintenance of records to reflect transactions and dispositions of assets;
- provide reasonable assurance that transactions are recorded to permit preparation of financial statements and that receipts and expenditures are properly authorized; and
- provide reasonable assurance regarding prevention or timely detection of unauthorized transactions.

(Securities Exchange Act of 1934 Rules 13a-15(f) and 15d-15(f))

Other SOX provisions support the protection of financial information in email as well. Compliance with SOX fundamentally requires that company executives take the necessary steps to protect company email and its contents.

SOX §302 requires that executives of a company must certify the accuracy of annual or quarterly reports. The signing officers are also responsible for establishing and maintaining internal controls and for disclosing to the company's auditors and the audit committee of the board of directors all significant deficiencies in internal controls as well as any fraud that involves management of or other employees who have a significant role in the company's internal controls.

OX §802 requires accountants who audit or review a company's records are required to retain certain records for a period of seven years. If this information includes emails, the need for protection of the information in the email during transport and at a remote site outside of the company, such as an auditor's data system, is essential.

SOX § 501(a) requires securities analysts to be separated from broker/dealers by "appropriate informational partitions". It also restricts prepublication approval of research reports by investment banking. Investment banks may face requests to provide evidence of any email interactions between these two groups prior to publication of a report. To ensure that e-mails are not read by inappropriate parties, it is important to have e-mail encryption in place.

Liability for Breach of SOX

Liability for breach of SOX can be severe. Violation of the provision in SOX will be treated as a violation of the Securities Exchange Act of 1934, with the same penalties (SOX Section 3(b)(1)). The following are some examples of the liability that company executives and companies face for failing to comply with SOX:

The Securities and Exchange Commission may seek equitable relief from officers and directors or a company in any action or proceeding brought or instituted by the SEC in federal court (SOX § 305).

If a company has to prepare an accounting restatement due to the material noncompliance of the company, as a result of misconduct, with any financial reporting requirement, the chief executive officer and the chief financial officer of the company may have to reimburse the company for any bonus or other incentive-based compensation received by that person from the company in the twelve month period the first public issuance or filing with the SEC.

Criminal penalties have also been established for certifying a periodic financial report knowing that the information contained in the report does not fairly represent the financial condition of the company. These penalties may result in imprisonment for a maximum of 20 years and or a fine of up to \$5,000,000 (SOX § 1106).

Criminal penalties also exist for altering or destroying documents, or otherwise impeding an official proceeding, which include imprisonment.

Example

The Securities and Exchange Commission charged the Senior Vice President of Information Technology at AmeriCredit's Fort Worth headquarters, with trading shares based on nonpublic information that he obtained via his computer at AmeriCredit's corporate headquarters. As a result, the defendant avoided approximately \$41,763 in losses that he would have incurred by selling his AmeriCredit shares after the market had reacted to the information once it was released. The defendant settled with the SEC, paying an amount disgorging the defendant of the gain, as well as interest and civil penalties.

(source: SEC statement of claim: *Sec v. James M. Adelt, et al.*, November 3, 2003)

The Gramm-Leach-Bliley Act

The Security Rules created under the Gramm-Leach-Bliley Act (GLBA) requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions (e.g. credit reporting agencies) that receive customer information from other financial institutions.

Who is affected?

The GLBA applies to “financial institutions” (i.e., businesses that are engaged in banking, insuring, stocks and bonds, financial advice and investing). The provisions regarding protection of consumers’ personal financial information apply not only to financial institutions that collect information from their own customers, but also to financial institutions, such as credit reporting agencies, that receive customer information from other financial institutions.

Why Encrypt Email?

The GLBA states that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ non-public personal information (GLBA § 501(a)).

The GLBA also requires all financial institutions to design, implement and maintain safeguards to protect customer information (GLBA § 501(b)). In particular, the financial institutions must establish standards that:

- insure the security and confidentiality of customer records and information;
- protect against any anticipated threats or hazards to the security or integrity of the records; and
- protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer

(GLBA § 501(b))

In “Financial Institutions and Customer Data: Complying with the Safeguards Rule”, the FTC gives the following guidance with respect to securing email communications: “Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as [...] encrypting sensitive customer information when it is transmitted electronically over networks or stored online.”

Liability for Breach of GBLA

The privacy provisions of the GLBA are enforced by various state and federal regulators depending on the nature of the financial institution. Violations of the GLBA can result in:

- the financial institution being liable for penalties of up to \$100,000 for each violation; and
- the officers and directors of the financial institution may be personally liable for a civil penalty of up to \$10,000 for each violation.
- In addition, some financial institutions (e.g., many banks and savings associations) will be regulated under section 8 of the Federal Deposit Insurance Act. Under this Act, penalties may include:
 - termination of FDIC insurance;
 - cease-and-desist orders barring policies or practices deemed in violation of the Act’s privacy provisions;
 - directors and officers of the institution can be removed from their management positions;
 - financial penalties for individuals of up to \$1,000,000 for an individual; and
 - financial penalties for financial institutions of 1% of the total assets.

Example

The Federal Trade Commission charged two mortgage companies with violating the agency's Gramm-Leach-Bliley Safeguards Rule by not having reasonable protections for customers' sensitive personal and financial information.

In an administrative action filed against Nationwide Mortgage Group, Inc. and its president, the FTC alleged that the mortgage broker failed to implement safeguards to protect its customers' names, social security numbers, credit histories, bank account numbers, income tax returns, and other sensitive financial information. Sunbelt Lending Services, Inc., also agreed to settle similar FTC charges. The settlement with Sunbelt bars future violations of the Safeguards Rule and requires biannual audits of Sunbelt's information security program by a qualified, independent professional for 10 years.

According to the FTC's complaints, both companies failed to comply with the Rule's basic requirements, including that they assess the risks to sensitive customer information and implement safeguards to control these risks. In addition, Nationwide failed to, amongst other things, train its employees on information security issues and monitor its computer network for vulnerabilities. Sunbelt also failed to oversee the security practices of its service providers and of its loan officers working from remote locations throughout the state of Florida.

(source: FTC press release: November 16, 2004: "FTC Enforces Gramm-Leach-Bliley Act's Safeguards Rule Against Mortgage Companies")

California SB 1386

The California Database Notification Act (SB 1386) came into effect on July 1, 2003. It requires that companies, in the event of a breach of the security system of a database containing personal information, to notify all California residents whose unencrypted personal information was in the database at the time of the breach that their personal information may have been compromised.

Encrypted Mail protects emails from any potential unauthorized disclosure and thus greatly reduces the likelihood of a breach of this type and the resulting liabilities under SB 1386.

Who is affected?

SB 1386 applies to any state agency, person or business that conducts business in California, and that owns or licenses computerized data that includes personal data and whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person (SB 1386 § 4(a)).

SB 1386 defines personal information as the combination of an individual's first name or initial and last name with one of the following:

- social security number;
- driver's license number or California Identification Card number; or
- account number, credit or debit card number, in combination with required security codes or passwords that would enable access to an individual's financial account.

(SB 1386 § 4(e))

Why Encrypt Email?

SB 1386 does not require notification of California residents in the breached database if either the name or the additional data in the database relating to the individual is encrypted.

Encrypted information is not "personal information" subject to SB 1386. Therefore, businesses can protect themselves from costly notification procedures by encrypting all personal information stored in databases, and as it is transmitted and received.

Liability for Breach of SB 1386

A person or business that does not provide notification that unencrypted personal data of California residents has been compromised can be:

sued for damages by any California resident whose personal data was breached (SB 1386 § 3(a));

subject to a class action law suit; and

subject to injunctive remedies.

(SB 1386 § 3(b))

Other Legislation

There exist many other laws which call for encryption of email that apply to U.S. companies that do business in the U.S. as well as internationally.

The FTC Act, for example, prohibits “unfair or deceptive acts or practices in or affecting commerce. Prohibited practices include deceptive claims that companies make about privacy, including claims about the security they provide for consumer information,” the testimony says. “The Commission has brought five cases against companies for deceptive security claims, alleging that the companies made . . . promises to take reasonable steps to protect sensitive consumer information. Because they allegedly failed to take such steps, their claims were deceptive.” (FTC Testifies on Data Security and Identity Theft, March 10, 2005)

Encrypted Mail

With Encrypted Mail, encrypting email is no longer an “unreasonable measure” which prevents companies from protecting confidential information stored in databases and transmitted electronically.

Encrypted Mail is a critical tool that helps companies to:

- comply with legislation
- reduce risk of liability
- protect against unauthorized disclosure of private and confidential information
- verify the identity of the sender of email
- verify the integrity of the content of email
- associate their brand with trusted communications