



National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Email Encryption and Signatures



CERT-MU

**National Computer Board
Mauritius**

Table of Contentss

1.0 Introduction.....	4
1.1 Purpose and Scope	4
1.2 Audience	4
1.3 Document Structure	4
2.0 Background.....	5
3.0 Signing and Encrypting Email Messages.....	6
4.0 OpenPrettyGoodPrivacy (OpenPGP).....	8
5.0 Secure/Multipurpose Internet Mail Extensions (S/MIME).....	10
6.0 Digitally Encrypting and Signing Email Using Thunderbird	11
6.1 Installing Enigmail.....	11
6.2 Creating public/private keys	11
6.3 Sending and receiving public keys.....	12
6.3.1 Sending your public key via email.....	12
6.3.2 Receiving a public key via email	13
6.3.3 Sending a digitally signed and / or encrypted email	13
6.3.4 Reading a digitally signed and / or encrypted email	14
6.3.4 Revoking your key	15
7.0 Digitally Encrypting and Signing Email Using Microsoft Outlook.....	16
7.1 Encrypting a single message using Outlook 2016 and 2013.....	16
7.2 Encrypting all outgoing messages using Outlook 2016 and 2013	16
7.3 Encrypting a single message using Outlook 2010	16
7.4 Encrypting all outgoing messages using Outlook 2010.....	16
7.5 Encrypting a single message using Outlook 2007	17
7.6 Encrypting all outgoing messages using Outlook 2007.....	17
7.7 Digitally sign a single message using Outlook 2016, 2013, 2010	17
7.8 Digitally sign all messages using Outlook 2016, 2013, 2010	18
7.9 Digitally sign an individual message using Outlook 2007.....	19
7.10 Digitally sign all messages using Outlook 2007	19
8.0 Conclusion	20
9.0 References.....	21

***DISCLAIMER:** This guideline is provided “as is” for informational purposes only.
Information in this guideline, including references, is subject to change without notice.
The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to provide advice to users who wish to send sensitive data by means of email.

1.2 Audience

The targeted audience for this document includes all email users who wish to send sensitive data by email.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background on email encryption and signatures.

Section 3 gives a view on existing encryption standards and cipher suites.

Section 4 discusses the OpenPrettyGoodPrivacy protocol.

Section 5 presents the Secure/Multipurpose Internet Mail Extensions protocol.

Section 6 provides the steps for digitally encrypting and signing email using Thunderbird.

Section 7 provides the steps for digitally encrypting and signing email using Microsoft Outlook.

Section 9 concludes the document.

Section 9 comprises a list of references that have been used in this document.

2.0 Background

Electronic mail (email) is feasibly the most widely used medium for exchanging business information over the Internet. Organizations often want to protect the confidentiality and integrity of some of their email messages, such as preventing the exposure of personally identifiable information in an email attachment. Email messages can be protected by using cryptography in various ways.

Most standard email protocols default to unencrypted user authentication and send email data in the clear (unencrypted). Sending this data in the clear may allow an attacker to easily compromise a user account and/or intercept and alter unencrypted emails. At a minimum, most organizations should encrypt the user authentication session even if they do not encrypt the email data itself. Encrypted user authentication is now supported by most standard and proprietary mailbox protocols.

The issues involved with encrypted and signed email data are more complex. Encrypting and signing email places a greater load on the organization's network infrastructure, may complicate malware scanning and email content filtering, and often requires significant administrative overhead. However, for many organizations the benefits of email encryption and signatures will outweigh the costs.

3.0 Signing and Encrypting Email Messages

Organizations often want to protect the confidentiality and integrity of some of their email messages, such as preventing the exposure of personally identifiable information in an email attachment. Email messages can be protected by using cryptography in various ways, such as the following:

- Sign an email message to ensure its integrity and confirm the identity of its sender.
- Encrypt the body of an email message to ensure its confidentiality.
- Encrypt the communications between mail servers to protect the confidentiality of both the message body and message header.

The first two methods, message signing and message body encryption, are often used together. For example, if a message needs to be encrypted to protect its confidentiality, it is usually digitally signed as well, so that the recipient can ensure the integrity of the message and verify the identity of the signer. Messages that are digitally signed are usually not encrypted if the confidentiality of the contents does not need to be protected.

The third cryptography method listed above, encrypting the transmissions between mail servers, is typically applicable only when two organizations want to protect emails regularly sent between them. For example, the organizations could establish a virtual private network (VPN) to encrypt the communications between their mail servers over the Internet. Unlike methods that can only encrypt a message body, a VPN can encrypt entire messages, including email header information such as senders, recipients, and subjects. In some cases, organizations may need to protect header information. However, a VPN solution alone cannot provide a message signing mechanism, nor can it provide protection for email messages along the entire route from sender to recipient. Because most email messages are protected individually by digitally signing and optionally encrypting them, this section focuses on the use of these methods. The most widely used standards for signing messages and encrypting message bodies are Open Pretty Good Privacy (OpenPGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME).

Both are based in part on the concept of public key cryptography, which involves a user having a pair of related keys: a public key that anyone can hold, and a private key that is held exclusively by its owner. Because public key cryptography is so computationally intense, it is

used sparingly in email security; symmetric key cryptography, which is much more efficient, is much more heavily used.

Symmetric key cryptography requires a single key to be shared between communicating parties, the sender and recipient of an email message. The process involves the sender generating a random key and encrypting the message with it using a symmetric key encryption algorithm. The sender then encrypts the symmetric key with a corresponding public key encryption algorithm using the recipient’s public key, and sends both the encrypted message and encrypted symmetric key together to the recipient.

This hybrid process uses public key encryption only to encrypt the symmetric key. Because only the intended message recipient holds the private key that is needed to recover the symmetric key, no other party can decrypt the message and read it.

Digital signature techniques rely on the creation of a digest or fingerprint of the information (i.e., the message being sent) using a cryptographic hash, which can be signed more efficiently than the entire message.

Organizations may wish to choose encryption schemes approved by government because these are well-tested and secure. Table 1 presents general recommendations for selecting cryptographic suites for protecting email messages.

Recommended Use	Cipher Suites
Highest Security	Encryption: Advanced Encryption Standard (AES) ¹¹ 128, 192, or 256-bit encryption Authentication & Digest: Digital Signature Standard (DSS) or RSA with a key size of 2048 bits or higher and SHA with a digest size of 256 bits (SHA-256) ¹²
Security and Performance	Encryption: AES 128-bit encryption Authentication & Digest: DSS or RSA with a key size of 1024 bits or higher and SHA-1
Security and Compatibility	Encryption: Triple Data Encryption Standard (3DES) ¹³ 168/112-bit encryption (note: 3DES is considerably slower than AES) Authentication & Digest: DSS with a key size of 1024 bits or higher and SHA-1
Authentication and Tamper Detection	Authentication & Digest: DSS with a key size of 1024 bits or higher and SHA-1 or SHA-256

Table 1 Recommended Cipher Suites

4.0 OpenPrettyGoodPrivacy (OpenPGP)

OpenPGP is a protocol for encrypting and signing messages and for creating certificates using public key cryptography. It is based on an earlier protocol, PGP, which was created by Phil Zimmerman and implemented as a product first released in June 1991. The initial PGP protocol was proprietary and used some encryption algorithms with intellectual property restrictions.

Many free and commercial products that use the OpenPGP standard are currently available. The software can be downloaded or purchased from a variety of Web sites. Some OpenPGP-based products fully support the cryptographic algorithms such as 3DES and AES for data encryption, Digital Signature Algorithm (DSA) and RSA for digital signatures, and SHA for hashing.

Although certain aspects of OpenPGP do use public key cryptography, such as digitally signed message digests, the actual encryption of the message body is performed with a symmetric key algorithm. The following is a brief description of signing and encrypting a message with OpenPGP (some steps may occur in a different order):

- OpenPGP compresses the plaintext, which reduces transmission time and strengthens cryptographic security by obfuscating plaintext patterns commonly searched for during cryptanalysis.
- OpenPGP creates a random session key (in some implementations of OpenPGP, users are required to move their mouse at will within a window to generate random data).
- A digital signature is generated for the message using the sender's private key, and then added to the message.
- The message and signature are encrypted using the session key and a symmetric algorithm (e.g., 3DES, AES).
- The session key is encrypted using the recipient's public key and added to the beginning of the encrypted message.
- The encrypted message is sent to the recipient.

The recipient reverses the steps to recover the session key, decrypt the message, and verify the signature. Popular mail clients such as Mozilla Thunderbird, Apple Mail, Eudora, and Microsoft Outlook require the installation of plug-ins to enable the user to send and receive

OpenPGP-encrypted messages. The OpenPGP distribution sites listed earlier in this section contain instructions on how to use OpenPGP with various mail client applications.

There are also security gateway servers available that can use OpenPGP to encrypt, decrypt, sign, and verify signatures on email messages on behalf of users. If two organizations exchanging emails both use compatible security gateway servers, then the use of OpenPGP is essentially transparent to users. If only one organization has such a gateway, it can still be used to protect messages, but it is not a transparent process at all to users at other organizations. If a gateway user sends an email to a recipient at another organization, that recipient will actually receive a notification email from the gateway that explains how to retrieve the protected email, typically through an SSL-encrypted HTTP session. Some gateways can also perform these functions for emails sent to lists of users. For example, a single user could send an encrypted and signed email to a mailing list address. The gateway would decrypt the email and re-encrypt it for all the individual recipients of the mailing list. Each recipient can then decrypt the email and verify the original signature.

5.0 Secure/Multipurpose Internet Mail Extensions (S/MIME)

S/MIME, which was originally proposed in 1995 by RSA Data Security, Inc., is based on their proprietary Public Key Cryptography Standard (PKCS) #7 for data format of encrypted messages, and the X.509 version 3 standard for digital certificates.

S/MIME version 3 was developed by the IETF S/MIME Working Group, which now coordinates all development of the S/MIME standard adopted as an IETF standard in July 1999.

S/MIME version 3 is specified by the following RFCs:

- Cryptographic Message Syntax (RFC 3852)
- S/MIME Version 3 Message Specification (RFC 3851)
- S/MIME Version 3 Certificate Handling (RFC 3850)
- Diffie-Hellman Key Agreement Method (RFC 2631)
- Enhanced Security Services for S/MIME (RFC 2634).

The most significant feature of S/MIME is its built-in and nearly “automatic” nature. Because of heavy industry involvement from manufacturers, S/MIME functionality exists with default installations of common mail clients such as Mozilla and Outlook Express.

The actual process by which S/MIME-enabled mail clients send messages is similar to that of OpenPGP.20 S/MIME version 3.1 supports two symmetric key encryption algorithms: AES, which is recommended but optional for compliant implementations to support, and 3DES, which is mandatory for implementations to support. Organizations using S/MIME to protect emails should use AES or 3DES (preferably AES, which is considered a stronger algorithm than 3DES).

As with OpenPGP, there are security gateway servers available that can use S/MIME to encrypt, decrypt, sign, and verify signatures on email messages on behalf of users. Many of these gateways actually support both OpenPGP and S/MIME.

6.0 Digitally Encrypting and Signing Email Using Thunderbird

To use PGP within Thunderbird, Enigmail must first be installed.

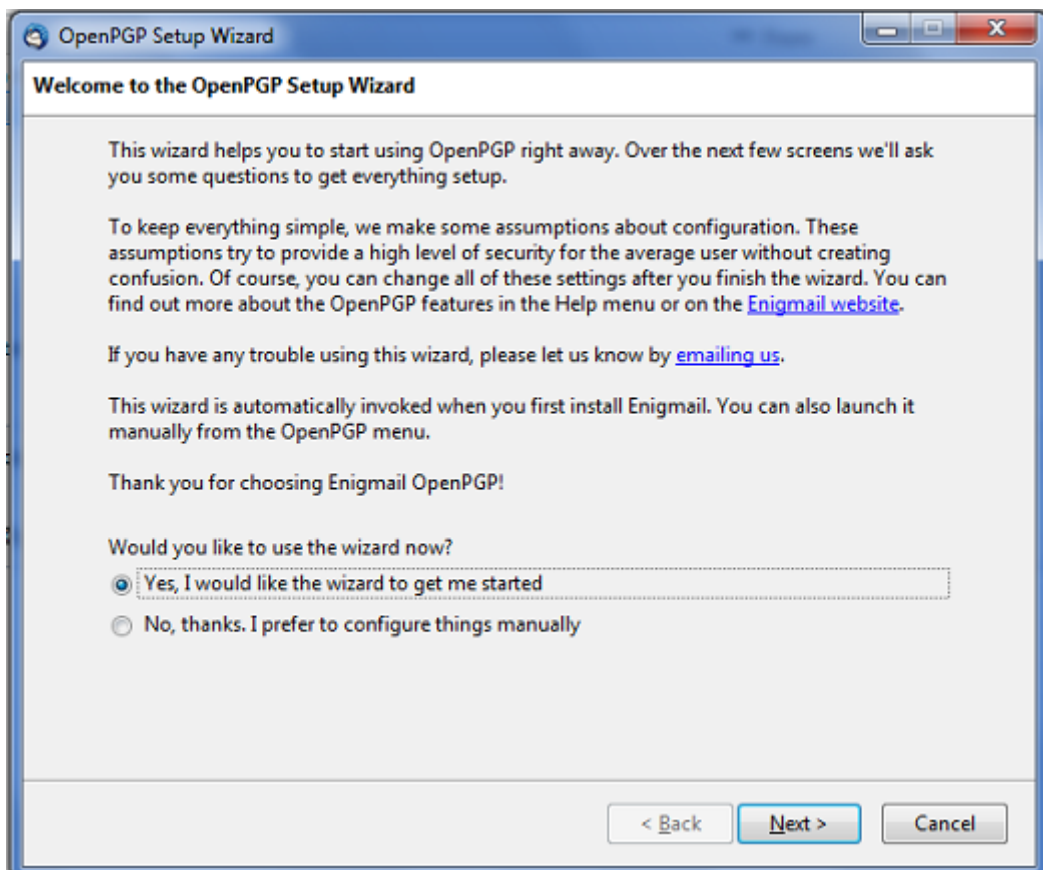
6.1 Installing Enigmail

To install Enigmail (On Windows):

1. In Thunderbird, select Tools > Add-ons.
2. Use the search bar in the top right corner to search for Enigmail.
3. Select Enigmail from the search results and follow the instructions to install the add-on.

6.2 Creating public/private keys

1. On the Thunderbird menu bar, click OpenPGP and select Setup Wizard.
2. Select Yes, I would like the wizard to get me started as shown in the image below. Click Next to proceed.



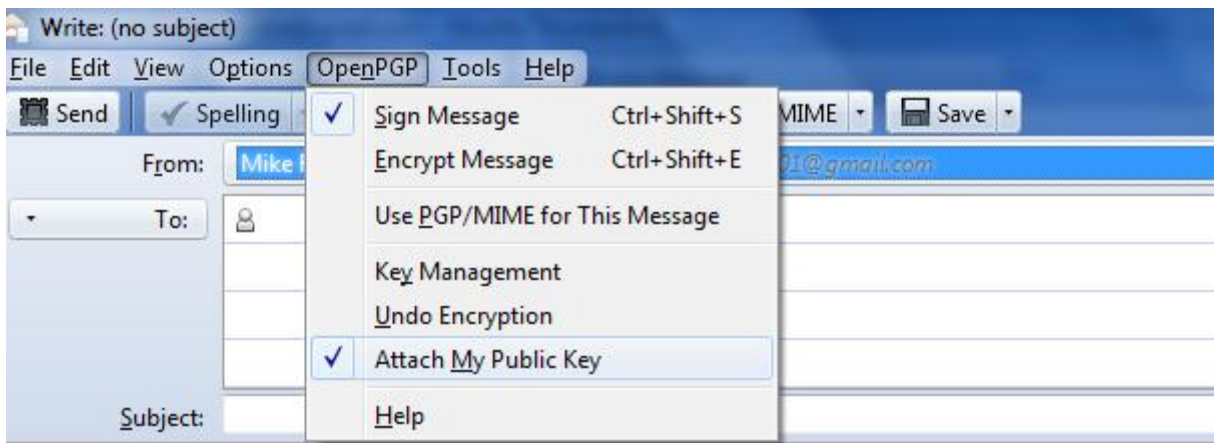
3. The wizard asks whether you want to sign all outgoing messages or whether you want to configure different rules for different recipients. It is usually a good idea to sign all emails so that people can confirm that the email is indeed from you. Message recipients do not need to use digital signatures or PGP to read a digitally signed message. Select Yes, I want to sign all of my email and click Next to proceed.
4. Next, the wizard asks if you want to encrypt all your emails. You should not select this option unless you have the public keys for all the people that you expect to send messages to. Select No, I will create per-recipient rules for those who send me their public keys and click Next to proceed.
5. The wizard asks if it can change some of your mail formatting settings to better work with PGP. It is a good choice to answer Yes here. Click Next to proceed.
6. Select the email account for which you want to create the keys. You need to enter a password in the 'Passphrase' text box which is used to protect your private key. This password is used to decrypt messages, so don't forget it. The password should be at least 8 characters long and not use any dictionary words. Enter this password twice and click Next to proceed.
7. The next screen displays the preferences you configured. If you are satisfied, click Next to proceed.
8. When the process of creating your keys is completed, click Next to proceed.
9. The wizard will ask if you want to create a 'Revocation certificate' which you would use if the security of your key pair was compromised and you needed to inform others that it is no longer valid. If you want to create the file click on Generate Certificate and follow the steps on the subsequent screens. Otherwise, click Skip.
10. The wizard finally informs you that it has completed the process. Click Finish to exit the wizard.

6.3 Sending and receiving public keys

6.3.1 Sending your public key via email

To receive encrypted messages from other people, you must first send them your public key:

1. Compose the message.
2. Select OpenPGP from the Thunderbird menu bar and select Attach My Public Key.

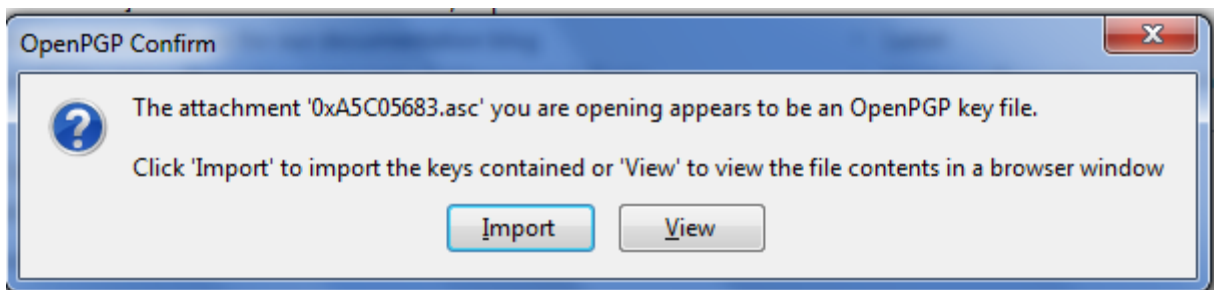


3. Send the email as usual.

6.3.2 Receiving a public key via email

To send encrypted messages to other people, you must receive and store their public key:

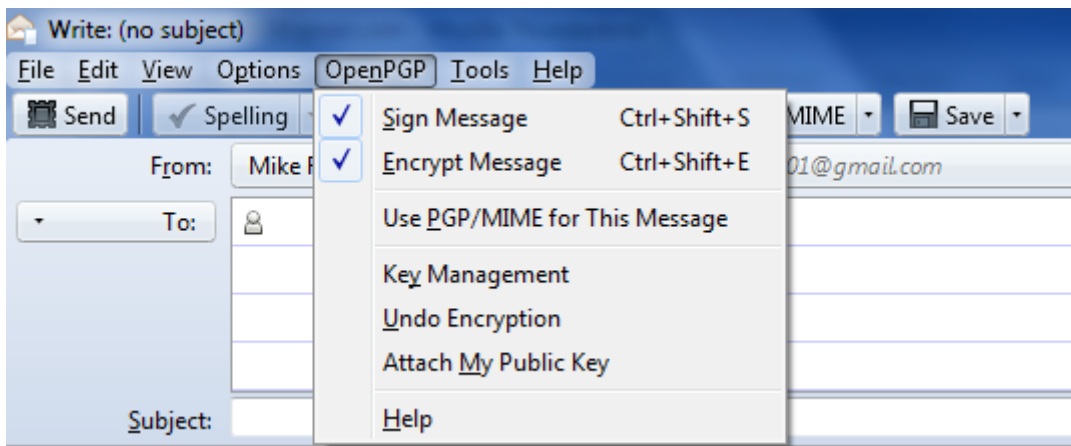
1. Open the message that contains the public key.
2. At the bottom of the window, double click on the attachment that ends in '.asc'. (This file contains the public key.)
3. Thunderbird automatically recognizes that this is a PGP key. A dialog box appears, prompting you to 'Import' or 'View' the key. Click Import to import the key.



4. You will see a confirmation that the key has been successfully imported. Click OK to complete the process.

6.3.3 Sending a digitally signed and / or encrypted email

1. Compose the message as usual.
2. To digitally sign a message, select OpenPGP from the Thunderbird menu and enable the Sign Message option. To encrypt a message, enable the Encrypt Message option. The system may ask you to enter your Passphrase before encrypting the message.



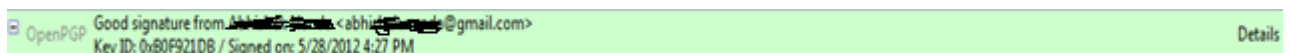
3. If your email address is associated with a PGP key, the message will be encrypted with that key. If the email address is not associated with a PGP key, you will be prompted to select a key from a list.
4. Send the message as usual.

Note: The subject line of the message will not be encrypted.

6.3.4 Reading a digitally signed and / or encrypted email

When you receive an encrypted message, Thunderbird will ask you to enter your secret passphrase to decrypt the message. To determine whether or not the incoming message has been signed or digitally encrypted you need to look at the information bar above the message body.

If Thunderbird recognizes the signature, a green bar (as shown below) appears above the message.



If the message has been encrypted and signed, the green bar also displays the text "Decrypted message".



If the message has been encrypted but not signed the bar would appear as shown below.

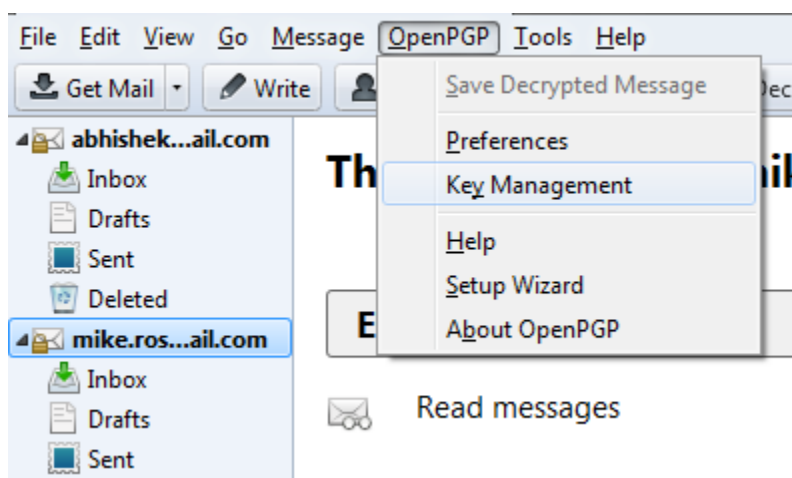


Note: A message which has not been signed could be from someone trying to impersonate someone else.

6.3.4 Revoking your key

If you believe that your private key has been "compromised" (that is, someone else has had access to the file that contains your private key), you should revoke your current set of keys as soon as possible and create a new pair. To revoke your current set of keys:

1. On the Thunderbird menu, click OpenPGP and select Key Management.



2. A dialog box appears as shown below. Check Display All Keys by Default to show all the keys.
3. Right-click on the key you want to revoke and select Revoke Key.
4. A dialog box appears asking if you really want to revoke the key. Click Revoke Key to proceed.
5. Another dialog box appears asking you to enter your secret passphrase. Enter the passphrase and click OK to revoke the key.

Send the revocation certificate to the people you correspond with so that they know that your current key is no longer valid. This ensures that if someone tries to use your current key to impersonate you, the recipients will know that the key pair is not valid.

7.0 Digitally Encrypting and Signing Email Using Microsoft Outlook

7.1 Encrypting a single message using Outlook 2016 and 2013

1. In message that you are composing, click **File > Properties**.
2. Click **Security Settings**, and then select the **Encrypt message contents and attachments** check box.
3. Compose your message, and then click **Send**.

7.2 Encrypting all outgoing messages using Outlook 2016 and 2013

When you choose to encrypt all outgoing messages by default, you can write and send messages the same as with any other messages, but all potential recipients must have your digital ID to decode or view your messages.

1. On the **File** tab, choose **Options > Trust Center > Trust Center Settings**.
2. On the **Email Security** tab, under **Encrypted email**, select the **Encrypt contents and attachments for outgoing messages** check box.
3. To change additional settings, such as choosing a specific certificate to use, click **Settings**.

7.3 Encrypting a single message using Outlook 2010

1. In the message that you're composing, on the **Options** tab, in the **More Options** group, click the dialog box launcher in the lower-right corner.
2. Click **Security Settings**, and then select the **Encrypt message contents and attachments** check box.
3. Compose your message, and then click **Send**.

7.4 Encrypting all outgoing messages using Outlook 2010

When you choose to encrypt all outgoing messages by default, you can write and send messages the same as you do with any other messages. All potential recipients, however, must have your digital ID to decode or view those messages.

1. On the **File** tab, click **Options > Trust Center > Trust Center Settings**.

2. On the **E-mail Security** tab, under **Encrypted e-mail**, select the **Encrypt contents and attachments for outgoing messages** check box.
3. To change additional settings, such as choosing a specific certificate to use, click **Settings**.

7.5 Encrypting a single message using Outlook 2007

1. In the message, on the **Message** tab, in the **Options** group on the ribbon, click the **Encrypt Message Contents and Attachments** button .
Note: If you don't see this button, click the **Options Dialog Box Launcher** in the lower-right corner of the group to open the **Message Options** dialog box. Click the **Security Settings** button, and in the **Security Properties** dialog box, select **Encrypt message contents and attachments**. Click **OK**, and then close the **Message Options** dialog box.
2. Compose your message and send it.


7.6 Encrypting all outgoing messages using Outlook 2007

Choosing to encrypt all outgoing messages means, in effect, your e-mail is encrypted by default. You can write and send messages the same as with any other e-mail messages, but all potential recipients must have your digital ID to decode your messages.

1. On the **Tools** menu, click **Trust Center**, and then click **E-mail Security**.
2. Under **Encrypted e-mail**, select the **Encrypt contents and attachments for outgoing messages** check box.
3. To change additional settings, such as choosing a specific certificate to use, click **Settings**.
4. Click **OK** twice.

7.7 Digitally sign a single message using Outlook 2016, 2013, 2010

1. In the message, on the **Options** tab, in the **Permission** group, click **Sign Message**.
 - If you don't see the **Sign Message** button, do the following:
 - In the message, click **Options**.

- In the **More Options** group, click the dialog box launcher  in the lower-right corner.
 - Click **Security Settings**, and then select the **Add digital signature to this message** check box.
 - Click **OK**, and then click **Close**.
 - If you don't see the **Sign Message** button, you might not have a digital ID configured to digitally sign messages, and you need to do the following to install a digital signature.
 - On the **File** menu, click **Options > Trust Center**.
 - Under **Microsoft Outlook Trust Center**, click **Trust Center Settings > Email Security**
 - Click **Import/Export** to import a digital ID from a file on your computer, or click **Get digital IDs** to find a list of services that issue digital IDs for your use.
2. Compose your message, and then send it.

7.8 Digitally sign all messages using Outlook 2016, 2013, 2010

1. On the **File** tab, click **Options > Trust Center**.
2. Under **Microsoft Outlook Trust Center**, click **Trust Center Settings**.
3. On the **Email Security** tab, under **Encrypted Mail**, select the **Add digital signature to outgoing messages** check box.
4. If available, you can select one of the following options:
 - If you want recipients who don't have S/MIME security to be able to read the message, select the **Send clear text signed message when sending signed messages** check box. By default, this check box is selected.
 - To verify that your digitally signed message was received unaltered by the intended recipients, select the **Request S/MIME receipt for all S/MIME signed messages** check box. You can request notification telling you who opened the message and when it was opened, When you send a message that uses an S/MIME return receipt request, this verification information is returned as a message sent to your **Inbox**.
5. To change additional settings, such as choosing between multiple certificates to use, click **Settings**.

6. Click **OK** on each open dialog box.

7.9 Digitally sign an individual message using Outlook 2007

1. In the message, on the **Message** tab, in the **Options** group, click the **Digitally Sign Message** button.
Note: If you don't see this button, click the **Options** dialog box launcher in the lower-right corner of the **Options** group to open the **Message Options** dialog box. Click the **Security Settings** button. and in the **Security Properties** dialog box, select the **Add digital signature to this message** check box. Click **OK**, and then close the dialog box.
2. Compose your message and send it.

7.10 Digitally sign all messages using Outlook 2007

1. On the **Tools** menu, in the Outlook Mail view, click **Trust Center**, and then click **E-mail Security**.
2. Under **Encrypted e-mail**, select the **Add digital signature to outgoing messages** check box.
3. If available, you can select one of the following options:
 - If you want recipients who don't have S/MIME security to be able to read the message, select the **Send clear text signed message when sending signed messages** check box. This check box is selected by default.
 - If you want to verify that your digital signature is being validated by recipients and to request confirmation that the message was received unaltered as well as receive notification telling you who opened the message and when it was opened, select the **Request S/MIME receipt for all S/MIME signed messages** check box. When you send a message with an S/MIME return receipt request, this verification information is returned as a message sent to your **Inbox**.
4. To change additional settings, such as choosing a specific certificate to use, click **Settings**.
5. Click **OK** twice.

8.0 Conclusion

The email infrastructure we all use is, by design, not secure. While most people connect to their email servers using a secure connection, some servers allow unsecured access. Additionally, as the message is transmitted from sender to recipient, the connections between each server are not necessarily secure. This makes it possible for third parties to intercept and temper with email messages. Hence, encryption and digital signatures are used to protect the confidentiality and integrity of email messages.

9.0 References

- www.nist.gov
- <https://support.mozilla.org>
- <https://support.office.com>