E-mail Encryption

by Sharon D. Nelson and John W. Simek

The most used method of electronically communicating today is via e-mail. Some may argue that text messaging is the number one method and that may be true for the younger generation, but businesses are generally communicating with some sort of e-mail service. The issue that we need to tackle is whether our electronic communications are secure (or need to be) and how to securely communicate when needed.

Attorneys have an ethical duty to protect the confidentiality of client information. It's not just the written word and paper documents. The duty extends to electronic communications as well. Sending a simple e-mail message potentially exposes the contents to interception by the bad guys if not our own government. Encryption can protect the electronic communications thereby preserving the confidentiality of the information. In addition, digitally signing communications helps ensure the authenticity of the sender. **Real Estate attorneys in particular** will benefit from encrypting e-mail and attachments, especially since they deal with a lot of financial and personally identifiable information. Since 47 states now have data breach notification laws, you don't want your law firm to need to comply with your state law because you didn't realize that e-mail encryption is now cheap, easy – and may start to be ethically required as a matter of competence. Using e-mail encryption when transmitting sensitive data has become a no-brainer.

Microsoft Exchange Server

By default, Exchange is configured automatically to attempt to communicate with other servers using TLS (Transport Layer Security), which is the successor to SSL. This means that the server-to-server communications travel in an encrypted state. You can also configure Exchange so that communications between two domains is required to be encrypted using TLS. If the same encryption level does not exist between the two domains, the messages are returned and a non-delivery report (NDR) is generated. Obviously, this would be a very secure configuration and something that may be considered for use between the firm and specific clients. However, implementing such configurations is best left to the technology professionals. We are pretty sure we won't see any attorneys attempting to do this on their own.

Exchange can also be configured to require TLS encryption for the accessing computers. This means that any software (e.g. Outlook) must use TLS in order to access a mailbox. Again, your IT person is probably better equipped to configure the TLS requirement for client computers.

E-Mail Encryption

This topic can be complicated and confusing for most lawyers. We'll try to simplify how to encrypt messages (and any attachments). The data flow is the same as if you were encrypting a file. Instead the "file" is an e-mail message.

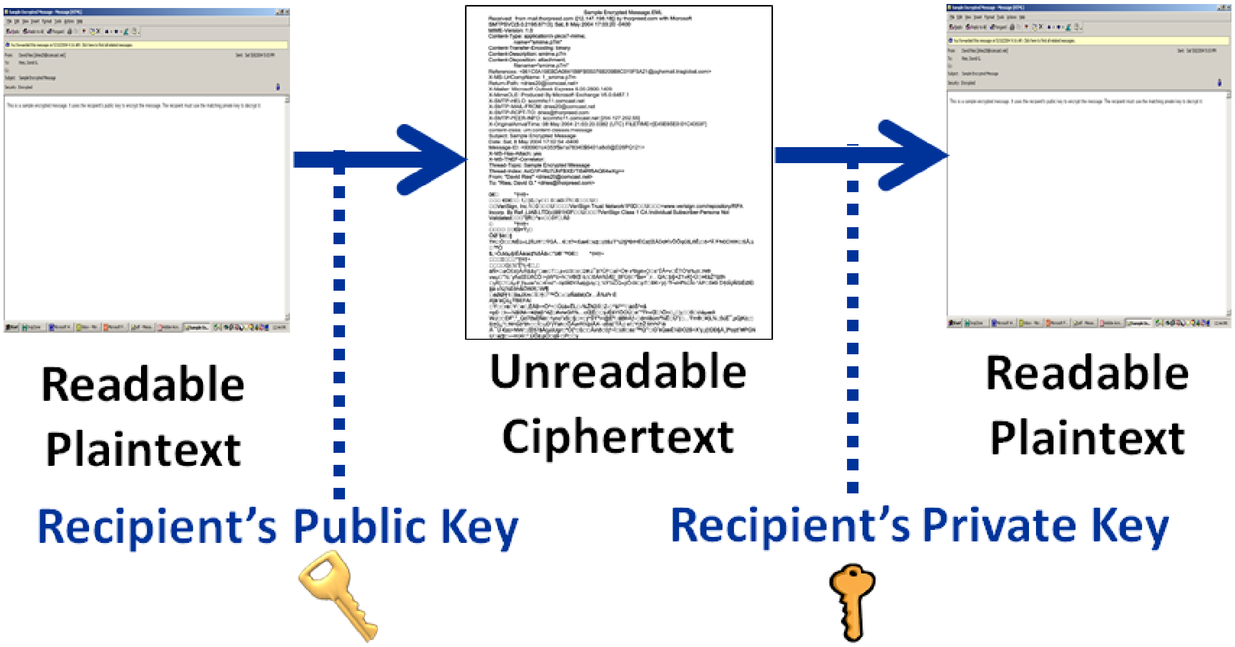


Figure 1

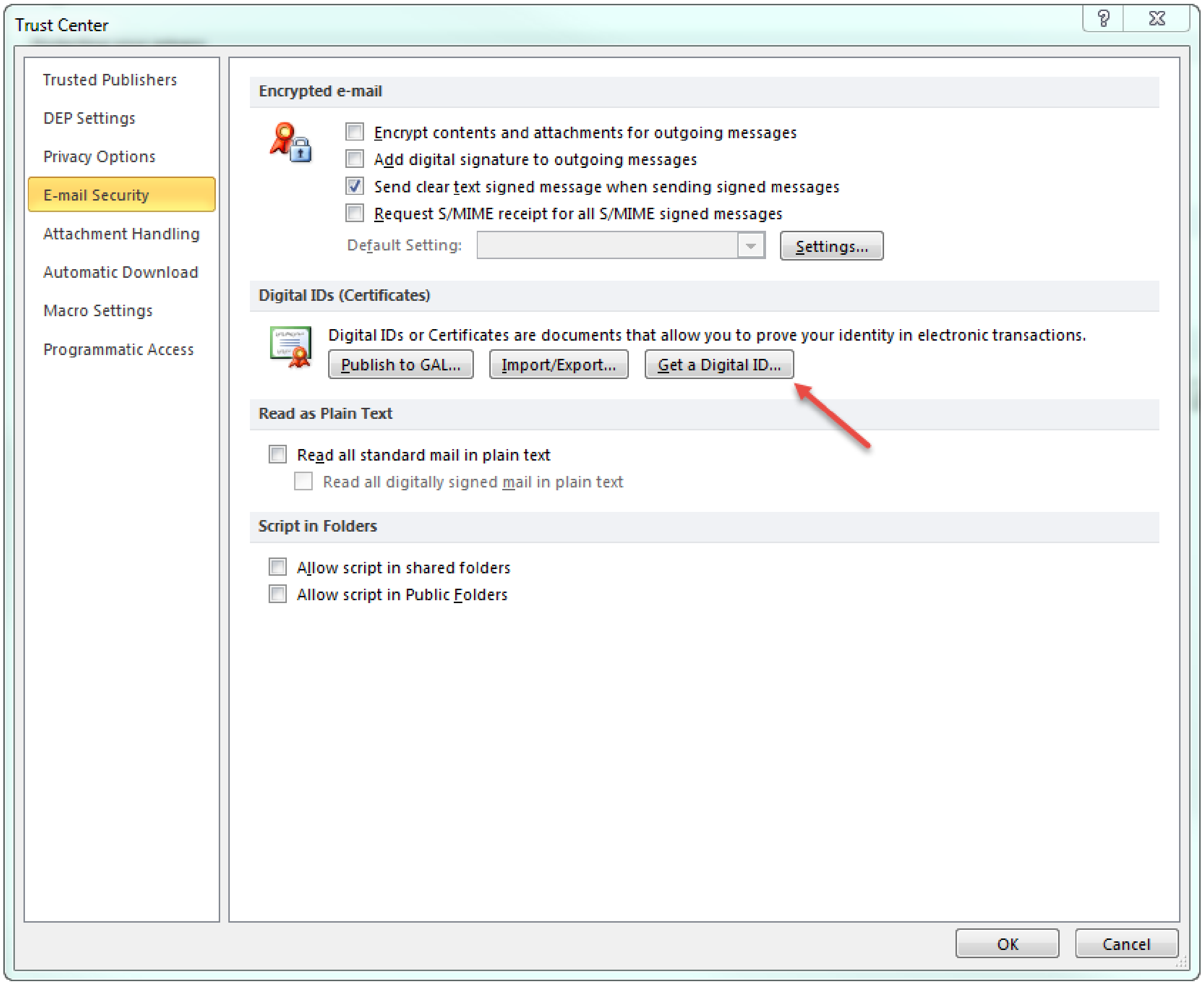
Figure 1 shows the steps (in simplistic form) for encrypting a single message. The sender starts by composing their e-mail message is plaintext. When they transmit the message the recipient's public key is used to encrypt the message with the output being unreadable ciphertext. The ciphertext (encrypted data) is sent along its merry way destined for the recipient. The recipient then uses their private key to decrypt the ciphertext into readable plaintext. The encryption applies to the message contents as well as any attachments.

As you can see, it is extremely important for the sender to have a copy of the recipient's public key in order to make this work. Key exchange and management is one of the challenges when trying to encrypt e-mail messages. Since the recipient is the only one with their private key (they better be the only one), that is used in decrypting the data, confidentiality is maintained.

Outlook Messages

Since the majority of attorneys use Outlook as their e-mail client, we'll describe the requirements and steps to encrypt a message when using Outlook. The first requirement is to have a digital ID, also known as a digital certificate. The digital ID helps prove your identity and includes the public and private keys needed for encryption. How do you get a digital ID? Just follow the steps below from Outlook:

1. Click on the **File** tab
2. Click **Options**
3. Click **Trust Center**
4. Under **Microsoft Outlook Trust Center**, click **Trust Center Settings …**
5. On the **E-mail Security** tab, under **Digital IDs (Certificates)**, click **Get a Digital ID …**



Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages
□ Add digital signature to outgoing messages
☑ Send clear text signed message when sending signed messages
□ Request S/MIME receipt for all S/MIME signed messages

Default Setting:

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Read as Plain Text

□ Read all standard mail in plain text
□ Read all digitally signed mail in plain text

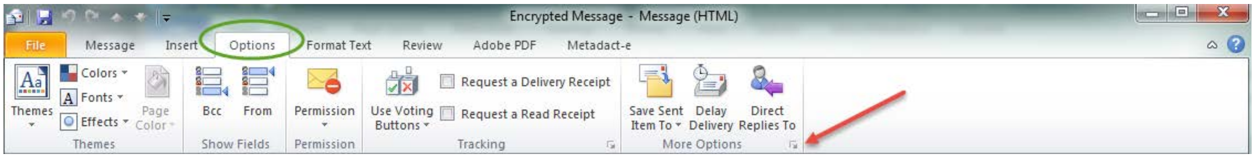
Script in Folders

□ Allow script in shared folders
□ Allow script in Public Folders

Figure 2

You will then open a browser window where you will have a choice to select a Digital ID provider. Once you have selected a provider and obtained your digital ID, follow the providers instructions on how to install the digital certificate to your computer.

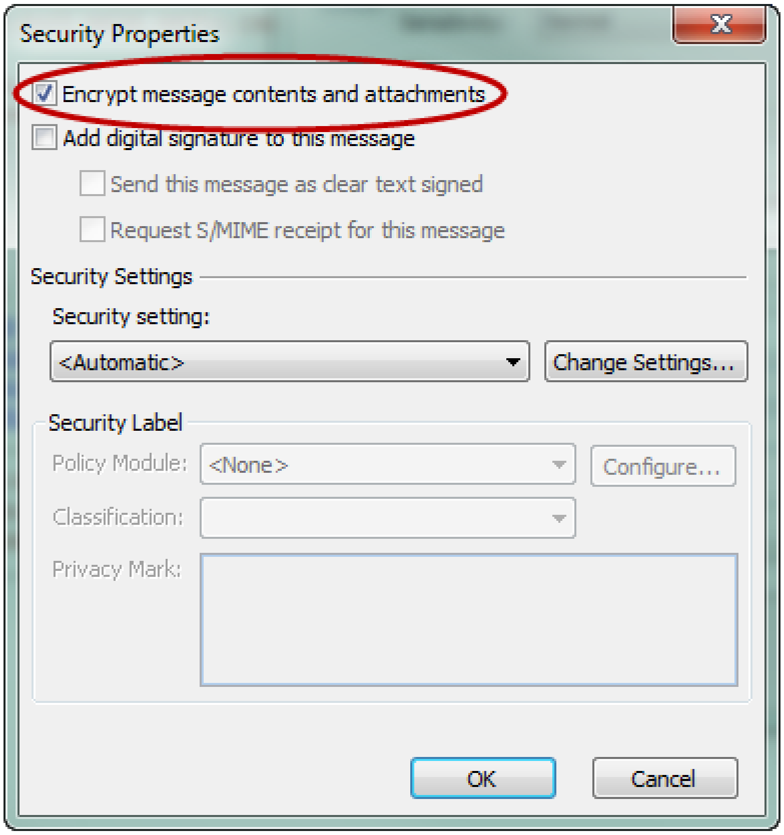
Once you have installed your digital ID, you can begin the process of sending an encrypted message from Outlook. Create your message and include any attachments you want to send along. Once you are ready to send the message, select the **Options** tab from the Ribbon and then the **More Options** symbol as shown by the arrow in Figure 3.



□ Request a Delivery Receipt
□ Request a Read Receipt

Figure 3

After selecting the **More Options** symbol, a **Properties** dialog box will be presented with additional options. Click on the **Security Settings …** button to display the **Security Properties** dialog box. Check the box for **Encrypt message contents and attachments** as shown in Figure 4 to encrypt the e-mail.



Security Properties

☑ Encrypt message contents and attachments

□ Add digital signature to this message

□ Send this message as clear text signed

□ Request S/MIME receipt for this message

Security Settings

Security setting: <Automatic>

Security Label

Policy Module: <None>

Classification:

Privacy Mark:

Figure 4

Remember we said previously that you need the public key of the recipient(s) in order to encrypt the message? If there is a problem with the certificate, therefore the key, you have the option of sending the message unencrypted by just clicking the **Send Unencrypted** button.

Secure E-mail Services

There are many providers of secure e-mail. Just do a Google search and all sorts of results will be returned. How do they work and what features are important? We can’t possibly cover all the solutions. ProtonMail (https://protonmail.ch/) gets high marks and good reviews. It is a complete end-to-end encrypted messaging system that does not require any installation. Other highly rated providers include 4SecureMail.com, ShazzleMail.com and StartMail.com. See if the vendor offers a trial period and if their system can integrate in your current e-mail environment with ease.

Hushmail

It would be impossible to discuss all the possible options for sending encrypted communications. One very popular service is called Hushmail. They have plans for Individuals, Business and HIPAA compliance. Hushmail is a web-based e-mail service that provides encrypted communications between parties. While

Hushmail encrypts e-mail, it is not a totally secure solution. The servers are located in British Columbia, Canada, and will comply with any lawful request to access the data. Under normal circumstances they do not store the passphrase that is used for encryption/decryption. However, it may be required to store a passphrase for an account identified in an order enforceable in British Columbia, Canada. Like the encrypted services of some cloud storage vendors, you need to understand that Hushmail does have the ability to access messages even though they are encrypted.

ZixCorp

Another service that is worth considering are the e-mail encryption services of Zix Corportation. ZixCorp is the only e-mail encryption provider with SOC3/SysTrust certification, SOC2 accreditation and PCI Level 1, DSS V2.0 certification. The encryption service is easy to install and very simple to use.

Most attorneys will subscribe to the ZixCorp service through a reseller. The reseller will set up the mail flow so that messages in and out are routed through the ZixCorp servers. This is similar to many spam and anti-virus services. The user installs an Outlook add-in that provides for one-button-click encryption. Compose your message and just click the button to encrypt. Simple, right? The message is then sent to the ZixCorp servers.

If the recipient can receive messages via a TLS connection, the message is delivered to directly to their Inbox and is opened it in Outlook with no further processing. If they do not have the ability to receive e-mail via TLS, they receive a link to the message on the ZixCorp servers. The recipient will have to create a login ID or login to their account if they have already created one. They then retrieve the message. In other words, a non-TLS enabled user will be viewing the decrypted messages via a web browser once they have logged in. It couldn't be easier.

If the message is delivered directly to the recipient's inbox, the recipient knows that the message was secured throughout its journey by the insertion of the ZixCorp graphic at the end of the message. This footer message is inserted by Zix for the e-mail that is delivered via a TLS connection. In addition, you have the option to set policies where the messages will automatically get encrypted based on message content. As an example, you can have a "financial policy," where Zix scans the e-mail for the inclusion of any financial data such as bank account numbers, credit card numbers, routing numbers, etc. If financial data exists then Zix will automatically encrypt the e-mail without the user clicking any buttons. You can override any policy by clicking on the Send Unencrypted button in the Outlook toolbar.

Would you use this all the time? Possibly, especially where there are a communications involving a real estate transaction. Items such as credit reports, deed transfers, closing documents, etc. could all be transmitted by e-mail if the attorney has encryption available.

Final Words

Encrypting e-mail is a very powerful tool for an attorney. Not only will encrypting e-mail fulfil your ethical duties to protect confidential client information, but it can save you money too. No more taking time to meet with clients to obtain signatures or pay courier fees to deliver closing documents. Pack the files as attachments to an e-mail message and encrypt away. Easy peasy. And cheap too.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com