Digital Signatures, Encryption, and the Secure Data Transfer Service

Introduction

IHS IT staff have received alerts that personnel have attempted to send email containing personally identifiable information without taking appropriate security measures, i.e. encrypting it or using the Secure Data Transfer Service (SDTS). This violates agency policy and our responsibility to protect the sensitive information of staff and the populations we serve. This tutorial provides guidance on why and how to digitally sign emails, encrypt them, and use the SDTS.

Please note the following:

Users can send and read any email encrypted with an IHS Personal Identity Verification, or PIV, card on the IHS email system as long as both users' PIV certificates are published to the IHS Outlook Global Address List (GAL). Such encrypted emails cannot be sent externally to any recipient, including at another Operating Division within the Department of Health and Human Services (HHS) or directly to a recipient at HHS.

In this case, users should use the IHS Secure Data Transfer Service, as described later.

Why Use Digital Signatures

When you digitally sign an email before sending it, the recipient gets two assurances: first, that you are the person who sent the message, and that the message was not tampered with in transit. Digital signatures, like physical signatures, are unique to the person signing and tied to their identity.

Digital signatures do not change the message contents, and do not protect it from interception, in which someone other than the intended recipient reads it. If the recipient wants to respond to the message, they need to digitally sign their response.

IHS email system users use their IHS PIV card and their Personal Identification Number, or PIN, to digitally sign messages.

To read digitally signed messages, publish your security certificates to Outlook's GAL. These certificates are tied to your identity. This video also shows you how to publish your certificates to the GAL, if necessary.

Why Use Email Encryption

Encryption converts the text of an email into an unreadable format, keeping unauthorized persons from viewing sensitive information. Email encryption often also provides authentication, another way of saying proof of identity.

Why Use SDTS

SDTS allows IHS employees to exchange sensitive data, including messages and large files, securely with recipients inside and outside of the IHS network in a Web application.

How to Digitally Sign a Message

In most cases, you can use the Sign button on Outlook's File tab to sign messages. If you attempt to complete the outlined steps, but the Sign button is not available on the File tab, contact [ITSupport@ihs.gov for assistance.](mailto:ITSupport@ihs.gov)

Log in to your workstation using your PIV Card and associated PIN.

Open Outlook and create a new message.

On the message window, select the Options tab to display its options.

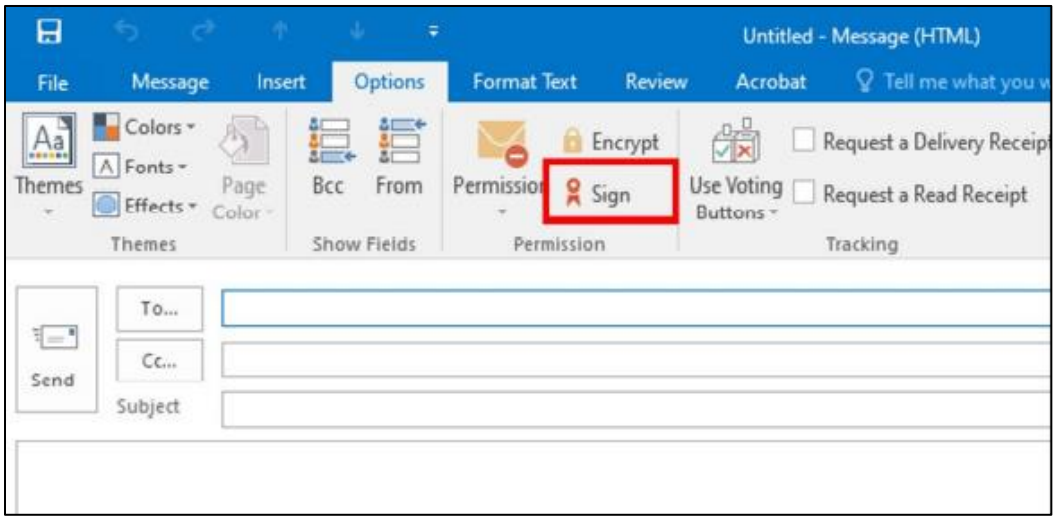

Figure 1 - Options Tab

Click on the Sign button in the Permissions section.

Fill in the To, Subject, and CC fields, and compose the message body as usual.

Click on the Send button. Outlook displays a Windows Security window, prompting you to enter your PIN.

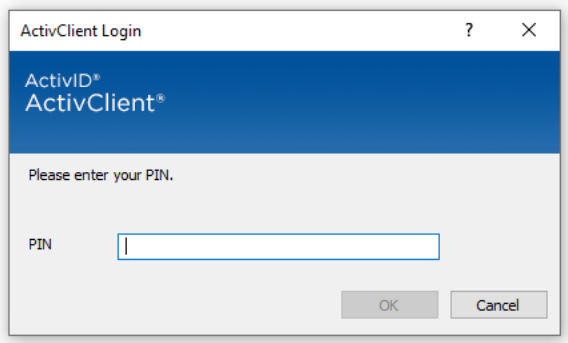

Figure 2 - Enter Your PIN

Complete the process by entering your PIN and clicking on the OK button. This sends the digitally signed message to all recipients.

How to Publish Digital Certificates to the Global Address List (GAL)

Digital certificates reside on PIV cards and are used to authenticate, or verify, your identity. When you get a new smart card with new digital certificates, Outlook usually imports the certificates from the card automatically. These certificates are required to read a digitally signed email.

Sometimes, a system does not import these certificates automatically. If yours does not, it will display the following message when you try to read a digitally signed email:

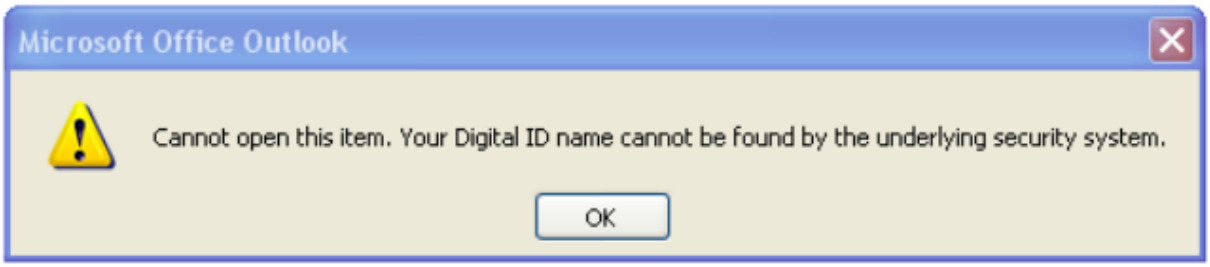

Figure 3 - Error Message When Lacking Certificates

If you receive this message, follow these steps to publish your digital certificates:

Access the Trust Center window in Outlook, as follows:

Click on the File tab and select Options from the navigation pane at the left of the screen to display the Outlook Options window.

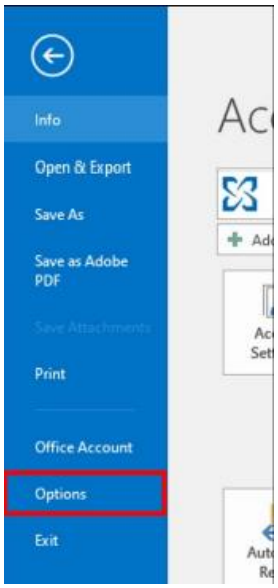

Figure 4 - Options on the Outlook File Tab

In the Outlook Options window, click on the Trust Center menu option, and then the Trust Center Settings button.

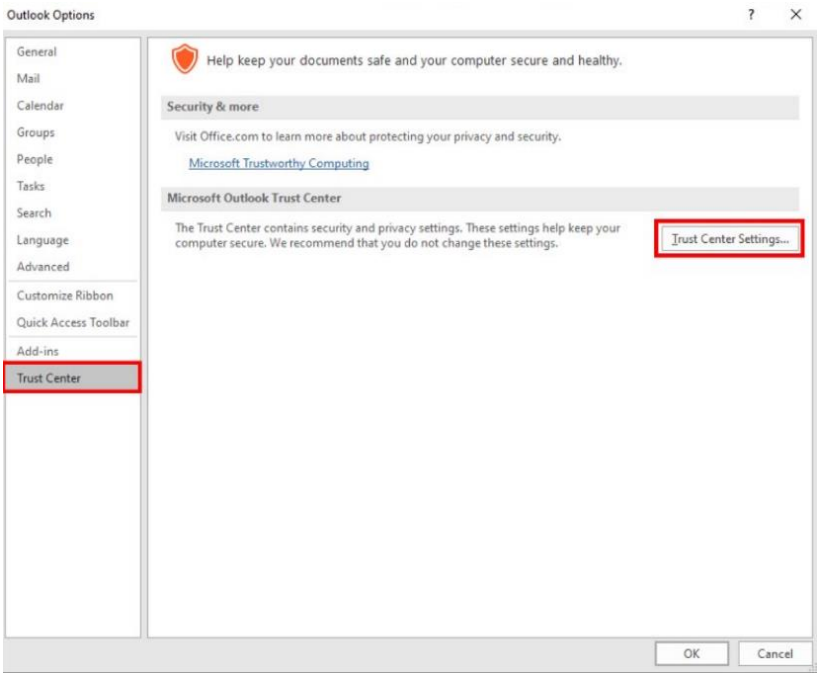

Figure 5 - Trust Center

In the Trust Center window, click on the E-mail Security link in the left pane to display its options in the right pane. In the Digital ID (Certificates) area, click on the Publish to GAL button, and then click on the OK button.

When the system prompts you to confirm publishing your security certificates to the Global Address List, click on the OK button.

When prompted, enter the PIN associated with your PIV card and click on the OK button. The system will display the message: Your certificates were published successfully.

Click on the Settings button and wait for the system to display your information in the Default Settings.

Click on the OK button to close the message and exit the Trust Center.

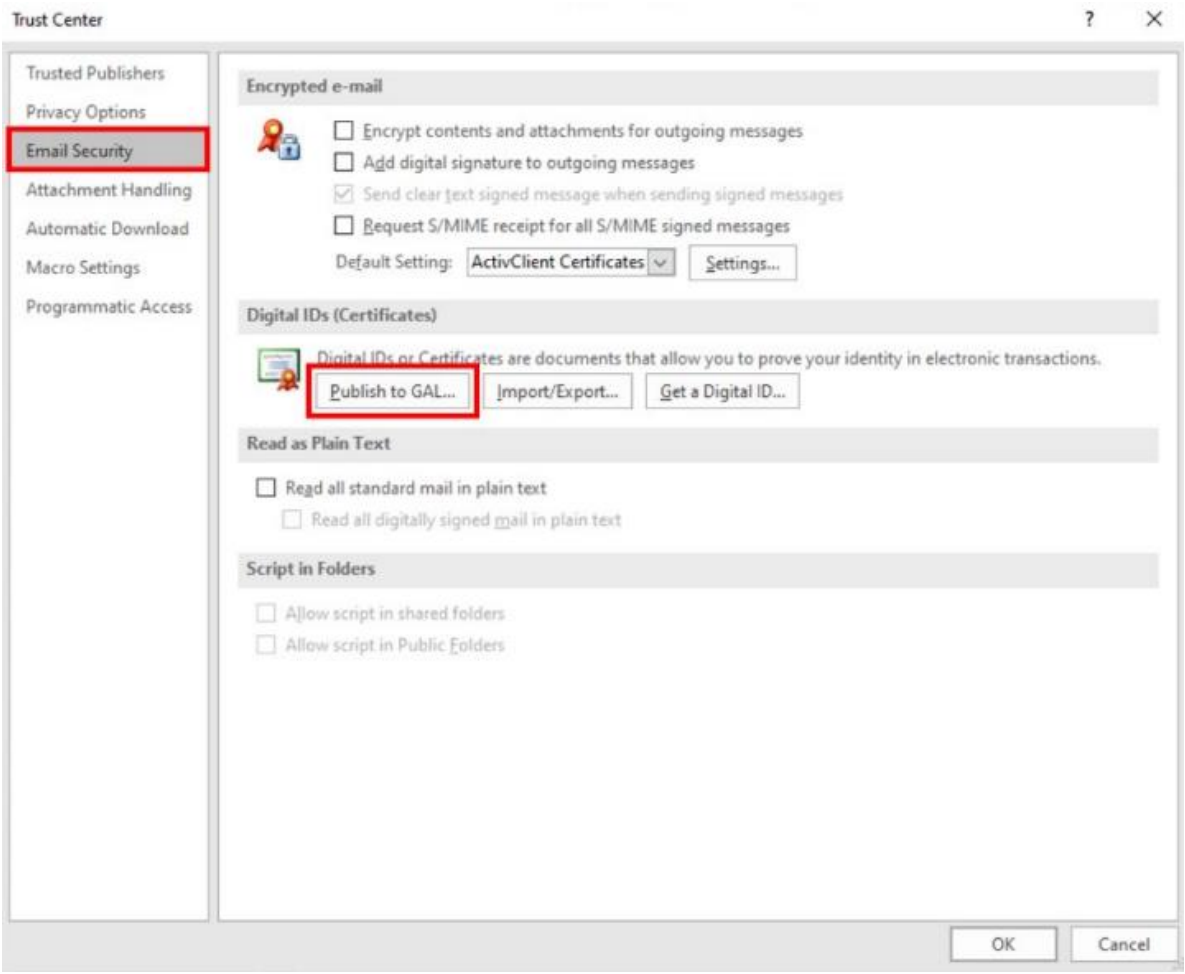

Figure 6 - Publish Certificates to GAL

How to Send an Encrypted E-Mail Message

IHS email users with a business need to send sensitive information are required to encrypt such information when transmitting it electronically. When sending it to another user within the IHS.gov email domain, use Outlook's encryption functionality, as described next.

Draft your email as usual.

Select the Options ribbon and click on the Encrypt button in the Permissions section.

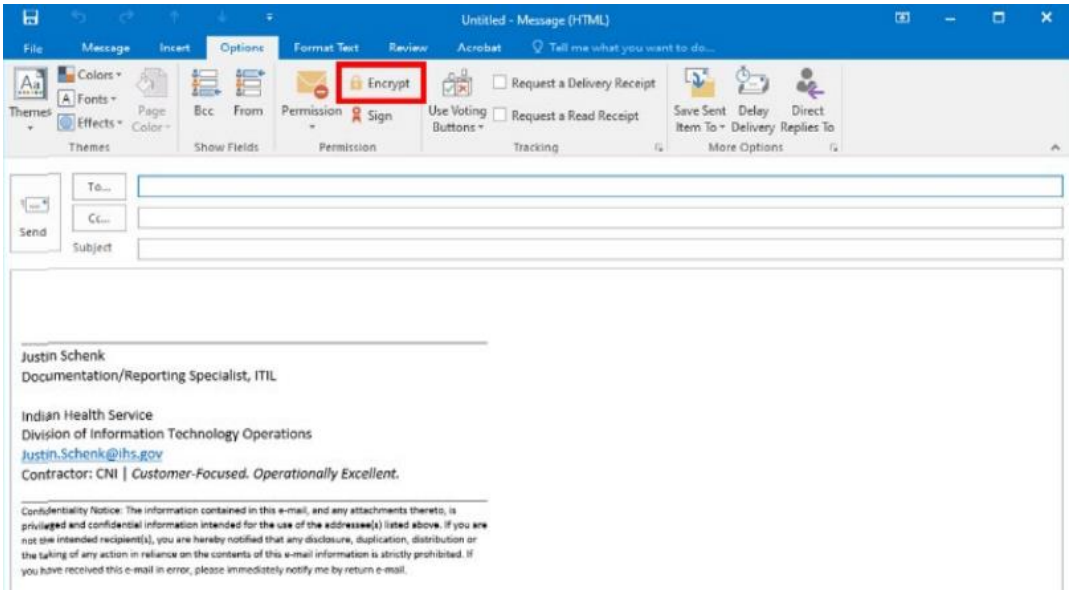

Figure 10 – Encrypt button

Click on the Send button and enter your PIN to send the encrypted message.

For more information on these digital signatures and email encryption, review the Division of Information Technology Operations Technical Note at https://home.ihs.gov/oittfs/.

If you receive an error that your certificates are missing or invalid, follow instructions on publishing your certificates in How to Add Digital Signatures and Encrypt E-Mails in Outlook, also found at https://home.ihs.gov/oittfs/

How to Send Secure Email Using SDTS

IHS email system users may have a business need to send sensitive information to others outside the IHS.gov email domain. They are still required to encrypt such information when transmitting it electronically and should use SDTS to do so.

To receive an SDTS transmission, users outside the IHS must complete a simple one-time registration process. The PDF document Using the IHS Secure Data Transfer Service explains the registration process, and can be used by all non-IHS recipients to whom you need to send encrypted e-mail or large files. Find this document at https://securedata.ihs.gov/sdts/custom/SendingIHSSecureData.pdf

Using your preferred internet browser, go to the IHS SDTS website at https://securedata.ihs.gov.

Click the 'Sign in with your IHS PIV Card' link and follow the prompts to access SDTS.

Figure 11 – SDTS PIV Card login link

Click on the Compose Delivery button.

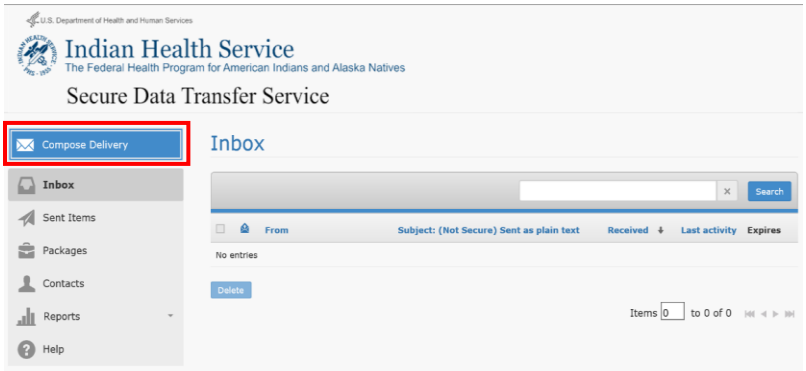

Figure 12 – Compose Delivery button

Complete the message details and attach any files you would like to send using the Attach files button.

Take special note of the field labeled 'Not Secure.' Any information in this field is sent as plaintext, so do not enter any sensitive information in it.

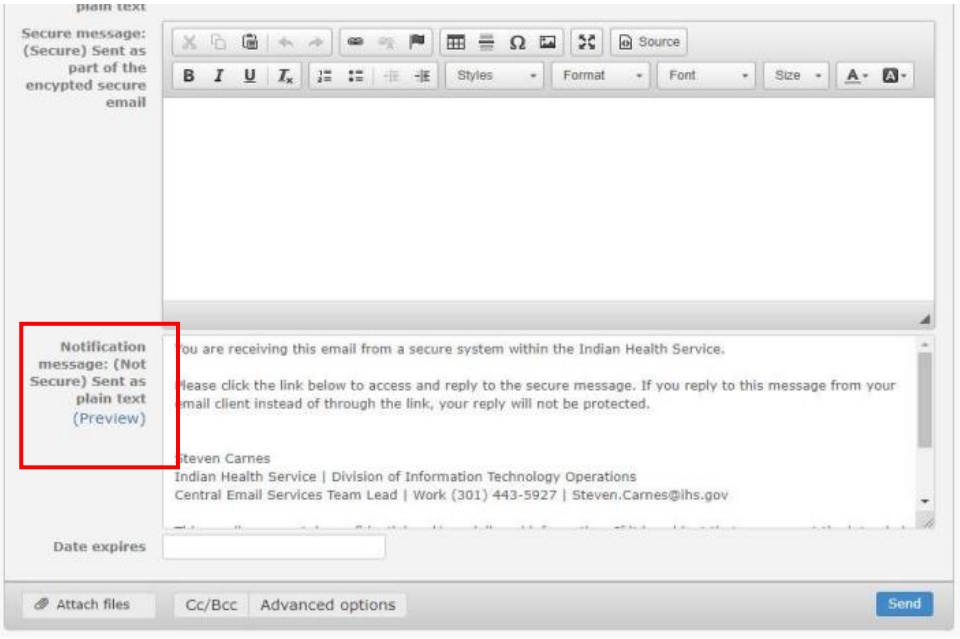

Figure 13 – SDTS Not Secure form field

Click Send to send the message. If you attached a file, an upload process will begin. You will then be prompted to optionally save the recipients of the message to your SDTS contacts list.

Resources

If you have any questions about this process, please contact cybersecurity@ihs.gov. For assistance with email encryption, SDTS, or digital certificates contact ITSupport@ihs.gov.

How to Add Digital Signatures and Encrypt E-Mails in Outlook (ihs.gov).

Using the IHS Secure Data Transfer Service