Setting Up a Digital Signature for IU Email

The steps include requesting and downloading the certificate, installing the certificate on your computer and/or iOS devices and configuring your mail client to use the certificate.

Requesting and downloading a S/MIME certificate

To get an S/MIME certificate for use at IU, fill out and submit the InCommon Certificate Manager S/MIME Certificate Enroll form (https://cert-manager.com/customer/InCommon/smime?action=enroll&swt=ac)

1. Use the following information to fill out the required fields (which are marked with asterisks):
    - **Access Code:** Enter clientcertsatiu
    - **First/Last Name:** Enter your legal name in the appropriate fields.
    - **Email:** Enter your primary IU email address (i.e., the address that appears in the IU Address Book and the Global Address List).
    - **Certificate Type:** InCommon Standard Assurance Client Certificate will autofill
    - **Pass-phrase:** Enter (and re-type to confirm) a passphrase for revoking your certificate or requesting a new one. **Important:** Do not use your Network ID passphrase. Do not forget this passphrase; use a password management tool, or save the passphrase in a secure location.
2. When you're finished, click Enroll. A "Validation Email" message from Certificate Services Manager (support@cert-manager.com) will be sent to the email address you entered on the enrollment form. The message contains instructions and a link for completing the enrollment process.
3. Click the link in the validation email to open the Account Validation form in your browser. The fields for your request code and email address will be automatically filled (and cannot be changed).
4. For "PIN", enter a strong passphrase (different from the passphrase you used in step 1, and from your Network ID passphrase), and then re-type it to confirm that you know it. Do not forget this PIN (use a password management tool, or save it in a secure location). **The PIN is used to encrypt your certificate, and you need it to install your certificate and private key.**
5. Optionally, select any automatically filled address fields to remove from the certificate. (ex. Address 1 and Address2)

6. When you're finished, click Validate, but do **not** close the web page. The InCommon Certificate Manager will process your request and display a Download button on that page. (You may need to wait a minute or longer for the request to be processed and the Download button to appear.)
7. Click Download to download the certificate.
8. Save the Digital Certificate to your desktop. Make a copy of the certificate to save to Box or the file server.

Your InCommon certificate will be encrypted in the PKCS 12 format (.p12 or .pfx) with the PIN passphrase you created on the Account Validation form. You need this PIN to install the certificate.

Note:

S/MIME certificates expire one year after creation (you may wish to set a reminder); see Renewing a certificate..

back to top

Installing the certificate to your Windows computer:

1. On the computer to which you're importing the certificate, locate your certificate file, right-click the file, and click Install PFX.
2. Current User will be selected, click Next.
3. File name will be filled in with certificate location, click Next.
4. Enter the PIN that you used to secure the private key, UITS recommends that you select Mark this key as exportable, leave Include all extended properties selected and click Next.
5. On the "Certificate Store" page, leave the default option Automatically select the certificate store based on the type of certificate. Click Next.
6. Click Finish. To complete importing your certificate, click OK.

back to top

Configuring Outlook 2016, 2013, and 2010 for Windows:

1. Open Outlook. From the File tab, choose Options, then Trust Center, and then Trust Center Settings.
2. Click Email Security.
3. Click Settings....
4. Next to the "Security Settings Name" text box, enter a name; this will simply be a label for your security settings, e.g., "My S/MIME Settings (username@iu.edu)".
5. Next to "Signing Certificate", click Choose.... Your certificate should be listed and click OK.
6. Next to "Encryption Certificate", click Choose.... Your certificate should be listed and click OK.
7. To digitally sign all your messages, check Add digital signature to outgoing messages, and click OK.
8. Click Publish to GAL to put your public certificate in the Global Address List. This will allow others at IU to access your public key so that they can send encrypted messages to you.
9. Click OK

back to top

Installing the certificate to your MacIntosh computer:

1. Double-click the file downloaded from the InCommon Certificate Manager.
2. OS X Keychain Access will prompt you for the certificate passphrase; enter the passphrase you created when you requested the cert (not necessarily your IU passphrase).

The certificate will be installed on your Mac and will appear in the "My Certificates" section of Keychain Access. The certificate is now available for Apple Mail, Outlook, and other applications that can use client certificates.

Note:
Your certificate is only available on the computer and user account where you install it. If you want your personal certificate on other computers or devices, you will need to export it.

Using your certificate with Apple Mail:

1. If you have just installed your certificate on your Mac, close Mail and then restart it.
2. Begin composing an email message. A "Signed" icon, containing a checkmark, should be in the lower right of the message header to indicate that the message will be signed. If the "Signed" icon does not appear, select Customize in the lower left of the message header and add the "Lock" and "Signed" icons.

Signing email

To send a signed message, verify that the "Signed" icon has a checkmark in it, and not an "x". If the "Signed" icon shows an "x", your message will not be signed.

You may not want to sign messages to mailing lists, because S/MIME digital signatures are attachments, which some lists do not accept.

Using your certificate with Outlook for OS X:

1. If you have just installed your certificate on your Mac, close Outlook and then restart it.
2. From the Outlook menu, select Preferences > Accounts. Select your IU email account, click Advanced, and then select the Security tab.
3. In the "Digital signing" section, select your certificate from the drop-down menu.
4. For "Signing algorithm", the default value of SHA-256 is appropriate for most situations.
5. For the best usability, enable the following options:
    - Sign outgoing messages
    - Send digitally signed messages as clear text
    - Include my certificates in signed messages
6. Click OK to save your changes and exit Outlook Preferences.

back to top

Using digital signatures for email on iOS devices:

1. From your computer, send yourself an email message with your certificate.p12 or certificate.pfx file as an attachment and copy and paste this URL to the message: http://cert.incommon.org/InCommonStandardAssuranceClientCA.crt
2. Install the "InCommon Standard Assurance Client CA" certificate on your iOS device; this allows your own certificate to appear as "Verified":
    1. On your iOS device, open the email you sent yourself and click the URL link in the message:

       ```
       http://cert.incommon.org/InCommonStandardAssuranceClientCA.crt
       ```

    2. On the "Install Profile" screen, you will see the "Verified" certificate file to install. Tap Install.
    3. If you are using Touch ID or have a passcode set up, you'll have to verify that to proceed. You may also see a notice informing you that installing the profile will change settings on your device. Tap Install when you're given the option.
    4. Tap Done.
3. On your iOS device, open the email message. Tap the attached file to start the installation.
4. On the "Install Profile" screen, tap Install.
5. If you are using Touch ID or have a passcode set up, you'll have to verify that to proceed. You may also see a notice informing you that installing the profile will change settings on your device. Tap Install when you're given the option.
6. You may see a warning that the profile is not signed, but tap Install and then Install again.
7. When prompted, enter the PIN for your certificate. Tap Next and then Done.

To check your profile, open the Settings app, then tap General, followed by Profiles. The certificate should have your name, and it should be checked as "Verified". If it's not, you may not have successfully installed the "InCommon Standard Assurance Client CA" certificate above.

Enabling client certificates for mail

1. Go to Settings > Mail, Contacts, Calendar > Select your email account > Choose Account which list your email address > Scroll to the bottom and click Advanced Settings.
2. Under S/MIME – slide to turn feature On
3. Sign – slide to turn On > Certificates – should have a check next to your name
4. Encrypt by Default > leave at No
5. Click the back arrow and then click Done

back to top

Using digital signatures for email on Android devices:

- To use S/MIME certificates on an Android device, you must be running Android OS 4.4 or later; still, your device may not support S/MIME certificates.
- You should already have your certificate file from InCommon on your personal computer. If you are unable to find your certificate file, you can export it from the certificate management application for your computer:
    - Exporting a certificate in Windows
    - Exporting a certificate in OS X

Installing the certificate

1. From your computer, send yourself an email message with your `certificate.p12` or `certificate.pfx` file as an attachment.
2. On your Android device, open the email message and tap the attached file to start the installation.
3. Enter the password for the certificate file, and tap OK.
4. When prompted for a certificate name, enter a name to use as a label for your certificate, for example `username@iu.edu`.
5. Next to "Credential use", make sure VPN and apps is selected.
6. To finish installing the certificate, tap OK.

To check your certificate, go to Settings > Security > Certificate Management > Trusted credentials, and then tap the User tab.

Note:
On Android devices, the following standard security notification may appear occasionally after installing new root certificates:

"A third party is capable of monitoring your network activity, including emails, apps, and secure websites. A trusted credential installed on your device is making this possible."

Enabling client certificates for mail

1. Go to Settings > Accounts > Microsoft Exchange > Email Settings.
2. Select the email account associated with your certificate.
3. Scroll down, and tap Security settings.
4. On the "Security Settings" screen, to digitally sign every message you send from your IU email account on this device, tap Signature.

back to top

Configuring Outlook 2016, 2013, and 2010 using IUanyWare:

1. Open Outlook. From the File tab, choose Options, then Trust Center, and then Trust Center Settings.
2. Click Email Security.
3. Click Import/Export button under Digital IDs (Certificates)
4. Import File: click the Browse button and select your digital certificate you downloaded
5. Password box, enter your PIN click OK.
6. Leave Security level set to Medium and hit OK
7. Next to the "Security Settings Name" text box, enter a name; this will simply be a label for your security settings, e.g., "My S/MIME Settings (username@iu.edu)".
8. Next to "Signing Certificate", click Choose.... Your certificate should be listed and click OK.
9. Next to "Encryption Certificate", click Choose.... Your certificate should be listed and click OK.
10. To digitally sign all your messages, check Add digital signature to outgoing messages, and click OK.
11. If you haven't done this already on your desktop PC, then click Publish to GAL to put your public certificate in the Global Address List. This will allow others at IU to access your public key so that they can send encrypted messages to you.
12. Click OK

back to top