

Lab Assignment 4

S/MIME and OpenPGP

1. Objective

In Lab 4, you will configure an email client to send encrypted and signed email, first using S/MIME and then using OpenPGP. Note that your S/MIME files, PGP keys, and passphrases to them are sensitive information. You should not lose these files, and keep them backed up in a secure location.

2. Software Installation

We have setup Ubuntu 16.04 virtual machines in Jetstream and used them for the labs so far. We will not be installing software in the virtual machines this time. You should, instead, use the host machine in Jetstream. You could use this lab exercise as an incentive to set up secure email on your personal laptop/desktops. You should install Mozilla Thunderbird email client:

<https://www.mozilla.org/en-US/thunderbird/>

Thunderbird is the suggested email program since it is available for all major desktop operating systems, for free. Details of configuring Thunderbird to use S/MIME certificates or OpenPGP keys might vary, depending on versions of software you are using. You will need to configure Thunderbird to send emails with your IU email address. The lab tasks require you to send signed and encrypted emails to the AI with your IU issued email address.

If you are not sure how to configure Thunderbird to send and receive email, the following articles will help:

<http://kb.iu.edu/data/awrr.html> (For IMail and UMail)

http://kb.mozillazine.org/Using_Gmail_with_Thunderbird_and_Mozilla_Suite

(For some UMail specific settings.)

You will have to use the account setup wizard when you run Thunderbird for the first time, or use Edit → Account Settings... → Account Actions → Add Mail Account. Settings will vary depending on whether you are signed up for imail or umail. We recommend that you skip the automatic configuration offered by Thunderbird, and use the manual setup. You will need to use

IMAP (with SSL or TLS) for receiving email, and SMTP (with TLS or STARTTLS) for sending email.

S/MIME support is built into Thunderbird. For OpenPGP, you will have to install Enigmail add-on for Thunderbird: Search → Type in 'enigmail' → Install → Restart

There are several OpenPGP compliant implementations. We will use GnuPG. Enigmail is a friendly frontend to GnuPG, but it doesn't install GnuPG on its own. You will have to install GnuPG separately, using one of the binaries (e.g., Gpg4win binary) listed at the download site, or using your Linux distribution's package manager.

<http://www.gnupg.org/download/>

3. Lab Tasks

3.1 S/MIME

At IU, S/MIME client certificates are provided by InCommon Certificate Service. You should follow instructions in this Knowledge Base article to procure an S/MIME client certificate:

<http://kb.iu.edu/data/bctk.html>

You will be required to use a passphrase, and you should not forget this passphrase or PIN. The certificate you will receive from InCommon will be encrypted in PKCS 12 format (a file with “.p12” extension), and the passphrase and PIN are needed to use this certificate. The file contains your public and private keys, and therefore should be kept secure. Before importing the certificate into Thunderbird, you must first set a master password for Thunderbird. The option for setting a master password is usually located under Menu → Options → Security → Passwords.

Once the master password has been set, you can import the certificate into Thunderbird, using certificate manager. The option for this is usually located under Menu → Options → Advanced → Certificates → View Certificates → Your Certificates → Import. You will be prompted to enter the master password for Thunderbird, and then the PIN and/or passphrase you chose for the certificate. To send an encrypted email to another person, you will need their S/MIME certificate, basically a “.cer” file. Similarly, in order for someone else to send an encrypted email to you, they will need to have your certificate. When you receive a signed message with a valid signature from someone, Thunderbird automatically adds their S/MIME certificates to the certificate manager.

You might notice that this poses a little chicken-and-egg problem. What if you need to send an encrypted message to someone before they have sent a signed message to you? Well, you can “manually” import their certificate into Thunderbird using the certificate manager.

3.1.1 Notes on using S/MIME certificates

How do you export a “.cer” file from your “.p12” file? One way would be using openssl pkcs12 command:

```
openssl pkcs12 -clcerts -nokeys -in [.p12 file] -out [.cer file]
```

What if the person(s) you want to communicate with are not affiliated with IU? One possibility is that they can use free personal certificates issued by one of the providers listed in this article:

http://kb.mozillazine.org/Getting_an_SMIME_certificate

3.1.2 What You Need to Do

You should download the S/MIME certificate (I520_AI.cer) from the files section, and import it into your Thunderbird instance, using certificate manager Menu → Options → Advanced → View Certificates → People → Import.

Set account settings to use your certificate for signing and encryption,

Options → Account Settings → [your account] → Security → Select your certificate for both the options (sign and encrypt) → Restart thunderbird

(Sometimes, after importing the certificate, it would seem that nothing has happened. Try restarting Thunderbird, and check security manager again.)

Next, you should send three emails to **dingchan@indiana.edu**:

- You should sign, but not encrypt, the first email, and the subject line should be “lab4_sd_SMIME-<your_username>”. In the message body, indicate that this is the signed email.
- You should sign and encrypt the second email, and the subject line should be “lab4_se_SMIME-<your_username>”. In the message body, indicate that this is the signed and encrypted email.
- You should encrypt, but not sign, the third email, and the subject line should be “lab4_e_SMIME-<your_username>”. In the message body, indicate that this is the encrypted email.

3.2 OpenPGP

As you have seen, S/MIME certificates are issued by a trusted third party. OpenPGP keys, however, are generated by you. Once the required software is installed, you should see an OpenPGP menu item in Thunderbird. OpenPGP → Setup Wizard will walk you through configuring OpenPGP.

You can accept the defaults, or change them according to your preferences. (You might not want to sign and encrypt all outgoing emails, for example.) You will be prompted for a key pair. If you already have generated a key pair, you can use that, or let the wizard guide you through this.

Extract your public key using Options → Enigmail → Key management → Right click on your key pair → Export keys to file → Export only public keys.

3.2.1 What You Need to Do

- Publish your public key with the two prominent public key servers:

<http://pgp.mit.edu/>

<http://keyserver.pgp.com/>

- Get the keys signed by at least one other students (the more, the merrier!) from the class. For signing, you will have to exchange key IDs and fingerprints. When you sign someone's key, you should verify that the key indeed belongs to the right person (e.g., through in-person communication). You should not sign a key if you are not sure about its origin. Once you sign someone's key, it is considered bad form to publish it yourself, instead, you should email the signed key to its owner, and let them publish it. If you are curious, there are detailed instructions on the web, on the "right" way of signing keys:

http://www.cryptnet.net/fdp/crypto/keysigning_party/en/keysigning_party.html

- Download the public key of dingchan@indiana.edu through the canvas link, and import it. The fingerprint (cryptographic hash) of the public key is 6C56 3CEE 25DB 9DED 1A22 1F6D 990A 7867 9283 07DF
- Now send three separate emails to **dingchan@indiana.edu**,
 - A signed, but not encrypted, email, with subject "lab4_sd_PGP-<your_username>", and indicate in the message body that it is a signed message.
 - A signed and encrypted email, with subject "lab4_se_PGP-<your_username>", and indicate in the message body that it is signed and encrypted.
 - An encrypted, but not signed, email, with subject "lab4_e_PGP-<your_username>", and indicate in the message body that it is encrypted.

4. Turn-ins

- Write a brief report of what you have done. In the report, include your OpenPGP key ID and signature. (Your public key will be downloaded from <http://pgp.mit.edu/> or <http://keyserver.pgp.com/> and checked for signatures.) Also, answer the question below:
 - Can you send signed/encrypted email using webmail such as Gmail? Why, or why not? What are the challenges?
- Explain what the key fingerprint is (mentioned in 3.2.1) and why you are convinced that this key is indeed Changchang's? Your argument should clearly indicate what properties of secure hash functions are important in making the decision.