Public-Key Infrastructure Lab

1. Overview

Public-Key Cryptography (PKI) is the foundation of modern digital communication. The problem is that there is no easy way to verify the ownership of a Public-Key. This lab is designed to demystify PKI and give students first-hand experience using PKI to send and receive encrypted digital messages and files. This lab covers the following topics:

- Public-Key
- Private-Key
- Public-Key Infrastructure (PKI)
- Publishing a Public-Key to a key server
- Validating a Public-Key
- Encrypting a message using an individual's Public-Key
- Decrypting a received message using your Private-Key

Learning Objectives

Students should be able to gain a better understanding of how PKI works and how it can be appropriately implemented and used to secure enterprise environments.

Readings

Additional detailed information about PKI can be found in the following:

- Chapter 7 – Cryptography and PKI in your TestOut e-book.
- Supplemental materials provided by your instructor.

Related Labs

None

Lab Environment

This lab has been tested using the environment listed below. Any variation outside this environment may cause certain aspects of this lab to not perform as indicated or desired.

- A Windows, macOS, or Chromebook laptop, or desktop computer.
- An e-mail account using Google's webmail platform G-Mail[1].
- The Firefox[2] web browser.
- The Mailvelope extension.
- An Internet connection.

[1] *The Mailvelope web browser extension is designed to work with different webmail platforms. This lab was written using G-Mail and is the preferred webmail platform for this lab. If you do not use G-Mail you can sign up for a free account by visiting https://gmail.com, and clicking on the "Create Account" hyperlink.*

[2] *This lab was written using the Firefox web browser and it is the preferred web browser for this lab.*

Ensure that you have created and/or logged into your G-Mail account before starting section two of this lab.

Read Ahead

You are required to submit a lab report for this lab. Read section three of this lab, review the requirements, you may need to take screenshots throughout each of the tasks in section two.

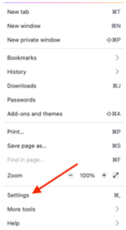
2. Lab Tasks

The following tasks and corresponding screenshots were written using the Firefox web browser and Google's webmail platform G-Mail. Deviation from the lab environment listed above is not recommended and may require outside research to complete this lab's tasks.

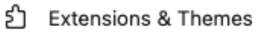
2.1 Task 1: Installing Mailvelope

In this task, we are going to install the Mailvelope extension on the Firefox web browser.

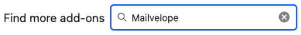
1. Open the Firefox web browser.
2. Click the sandwich ≡ icon located on the upper right of the Firefox browser window.
3. Click "Settings" from that menu; the "Settings" tab will appear.



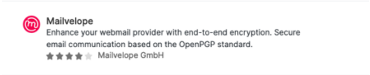
4. Click on the puzzle-piece icon "Extensions & Themes" located on the lower left of the "Settings" tab; the "Add-ons Manager" tab will appear.



5. In the "Add-ons Manager" tab, type "Mailvelope" into the "Find more add-ons" search box.

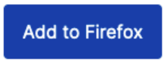


6. From the search results locate and click on Mailvelope, then click the "Add to Firefox" button to install the add-on.

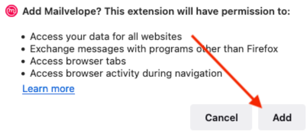

Mailvelope

Enhance your webmail provider with end-to-end encryption. Secure email communication based on the OpenPGP standard.

★★★★☆ Mailvelope GmbH



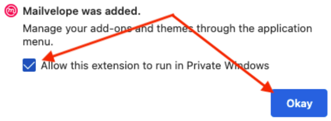
7. When prompted click the "Add" button to grant permission to the Mailvelope extension.



Add Mailvelope? This extension will have permission to:

- Access your data for all websites
- Exchange messages with programs other than Firefox
- Access browser tabs
- Access browser activity during navigation

8. Click the checkbox to permit Mailvelope in private windows, then click the "Okay" button.

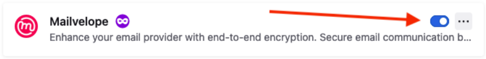


Mailvelope was added.

Manage your add-ons and themes through the application menu.

☑ Allow this extension to run in Private Windows

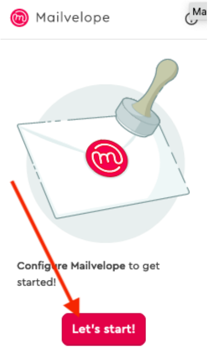
9. Return to the "Add-ons Manager" tab. Ensure that the Mailvelope extension is turned on.



Mailvelope

Enhance your email provider with end-to-end encryption. Secure email communication b...

10. Locate the Mailvelope icon located on the upper right of the Firefox browser window and click it to reveal the Mailvelope menu; click the "Let's start!" button.

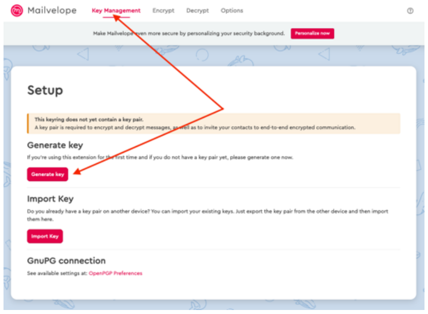


Configure Mailvelope to get started!

2.2 Task 2: Setup Mailvelope

In this task, you are going to set up the Mailvelope extension. You will start by generating a public/private key pair. Then you will validate your Public-Key by decrypting the e-mail sent to your G-Mail account by the Mailvelope key server. You will then export and upload your Public-Key to one (1) additional key server. Finally, you will export your public/private key pair to protect your keys from loss or corruption.

1. Click on the "Key Management" tab in Mailvelope. On the "Setup" screen, click the "Generate Key" button.



Make Mailvelope even more secure by personalizing your security background.

Setup

This keyring does not yet contain a key pair.
A key pair is required to encrypt and decrypt messages, as well as to invite your contacts to end-to-end encrypted communication.

Generate key

If you're using this extension for the first time and if you do not have a key pair yet, please generate one now.

Import Key

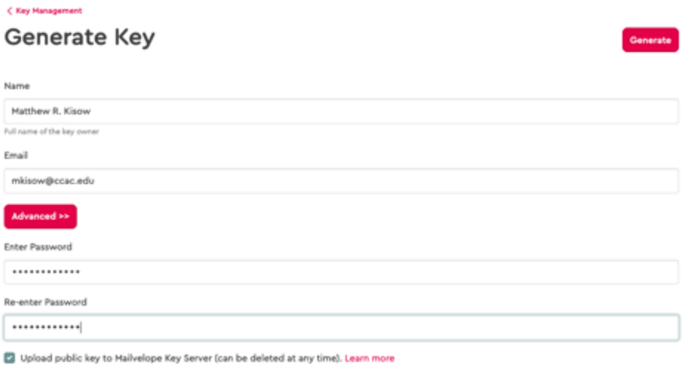
Do you already have a key pair on another device? You can import your existing keys. Just export the key pair from the other device and then import them here.

GnuPG connection

See available settings at: OpenPGP Preferences

2. On the "Generate Key" screen fill in the following information:

Name: Your Full Name
Email: Your G-Mail address.
Password: This is used to protect your Private-Key, ***DO NOT FORGET IT!***



Generate Key

Name
Matthew R. Kisow
Full name of the key owner

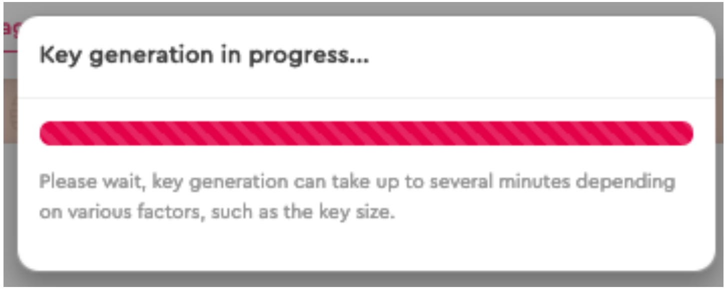
Email
mkisow@ccac.edu

Enter Password
••••••••••••

Re-enter Password
••••••••••••

☑ Upload public key to Mailvelope Key Server (can be deleted at any time). Learn more

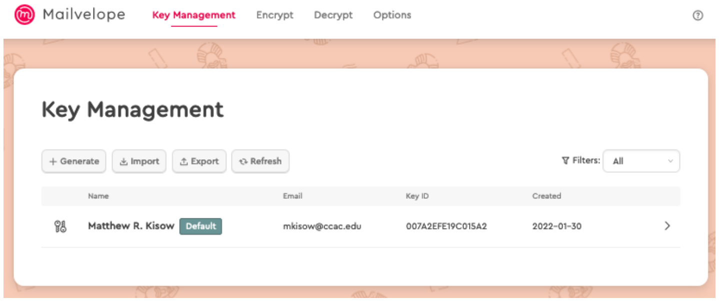
Ensure the "Upload public key to Mailvelope Key Server" checkbox is selected. Then click the "Generate" button, then wait while your key pair is generated.



Key generation in progress...

Please wait, key generation can take up to several minutes depending on various factors, such as the key size.

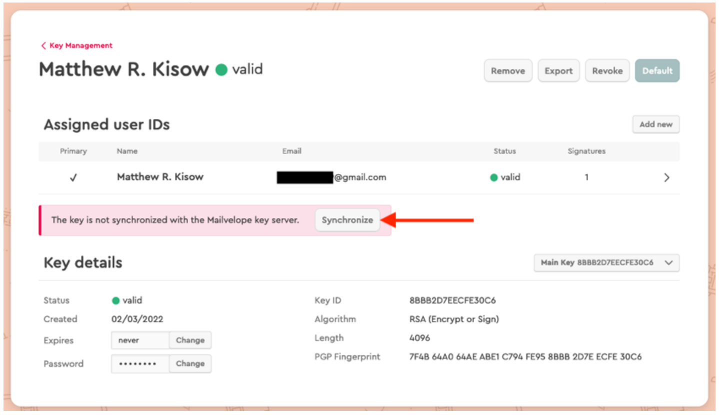
3. Upon successful key generation, you will be taken back to the "Key Management" screen in Mailvelope. Your new key will be listed with your name, e-mail address, the key's identifier, and the key's creation date.



Key Management

Name	Email	Key ID	Created
Matthew R. Kisow Default	mkisow@ccac.edu	007A2EFE19C015A2	2022-01-30

4. On the "Key Management" screen in Mailvelope, click on the right arrow next to your public/private key pair. You will be taken to your key pair details. If you see the message, "The key is not synchronized with the Mailvelope key server." Click the "Synchronize" button.



Matthew R. Kisow ● valid

Assigned user IDs

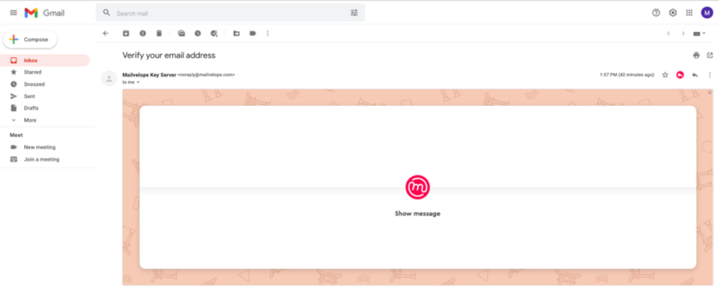
Primary	Name	Email	Status	Signatures
✓	Matthew R. Kisow	[redacted]@gmail.com	● valid	1

The key is not synchronized with the Mailvelope key server.

Key details

Status	● valid	Key ID	8BBB2D7EECFE30C6
Created	02/03/2022	Algorithm	RSA (Encrypt or Sign)
Expires	never	Length	4096
Password	••••••••	PGP Fingerprint	7F4B 64A0 64AE ABE1 C794 FE95 8BBB 2D7E ECFE 30C6

5. There should be a confirmation e-mail from Mailvelope[3] in your G-Mail inbox. This e-mail is encrypted and will look similar to the screenshot below. This e-mail contains a link to confirm your e-mail address.

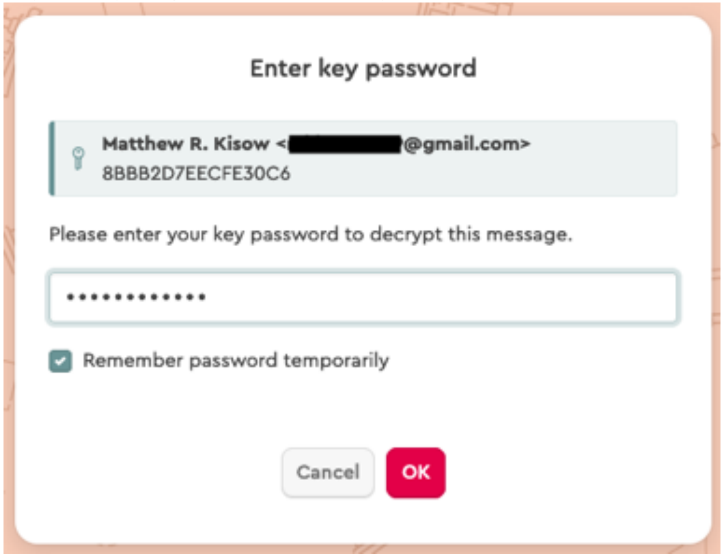


Verify your email address

Mailvelope Key Server <noreply@mailvelope.com>
to me
1:57 PM (42 minutes ago)

[3] *If you have more than one e-mail from Mailvelope, only click on the most recent one. If you are redirected to a page that states "User ID not found" follow the link from the other e-mail.*

6. From your G-Mail inbox, click on the e-mail from Mailvelope. You will be prompted in a separate window to enter your password; enter the password for your Private-Key that you generated in step two above. Then click the "OK" button.



Enter key password

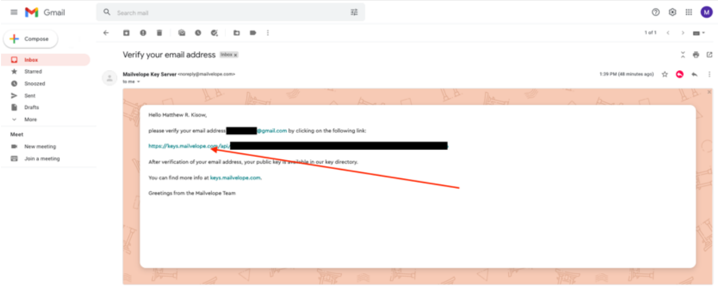
Matthew R. Kisow <[redacted]@gmail.com>
8BBB2D7EECFE30C6

Please enter your key password to decrypt this message.

•••••••••••••

☑ Remember password temporarily

7. Click the hyperlink from the decrypted e-mail to validate your e-mail address and to have your Public-Key listed on Mailvelope's global key servers.



Verify your email address Inbox

Mailvelope Key Server <noreply@mailvelope.com>
to me
1:39 PM (48 minutes ago)

Hello Matthew R. Kisow,

please verify your email address [redacted]@gmail.com by clicking on the following link:

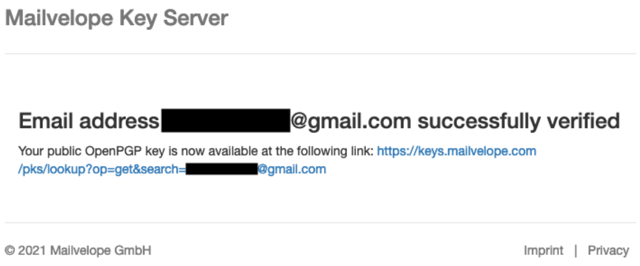
https://keys.mailvelope.com/api/[redacted]

After verification of your email address, your public key is available in our key directory.

You can find more info at keys.mailvelope.com.

Greetings from the Mailvelope Team

A successful message from the "Mailvelope Key Server" looks like this.



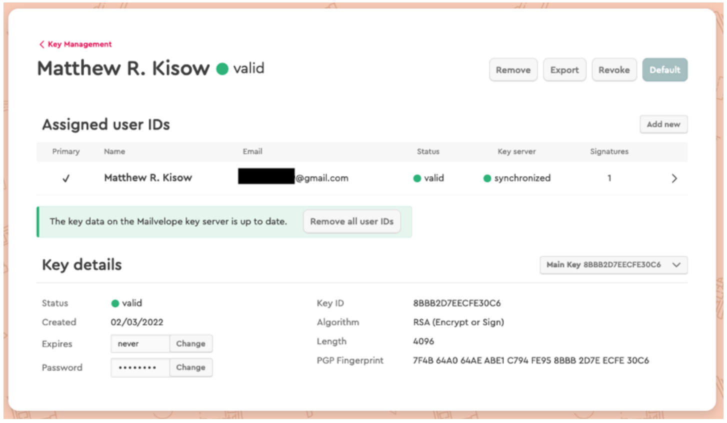
Mailvelope Key Server

Email address [redacted]@gmail.com successfully verified

Your public OpenPGP key is now available at the following link: https://keys.mailvelope.com/pks/lookup?op=get&search=[redacted]@gmail.com

© 2021 Mailvelope GmbH

8. Return to your key pair details on the “Key Management” screen in Mailvelope. You should now see the message, “The key data on the Mailvelope server is up to date.”



Matthew R. Kisow ● valid

Assigned user IDs

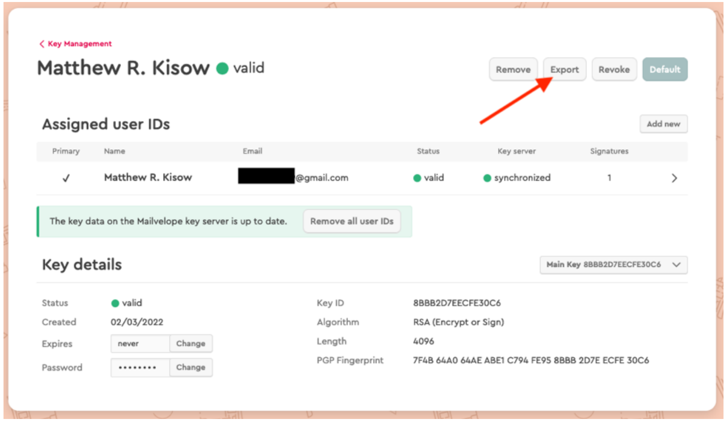
Primary	Name	Email	Status	Key server	Signatures
✓	Matthew R. Kisow	[redacted]@gmail.com	● valid	● synchronized	1

The key data on the Mailvelope key server is up to date.

Key details

Status	● valid	Key ID	8BBB2D7EECFE30C6
Created	02/03/2022	Algorithm	RSA (Encrypt or Sign)
Expires	never	Length	4096
Password	••••••••	PGP Fingerprint	7F4B 64A0 64AE ABE1 C794 FE95 8BBB 2D7E ECFE 30C6

9. From the key pair details screen in Mailvelope, click the “Export” button.



Matthew R. Kisow ● valid

Assigned user IDs

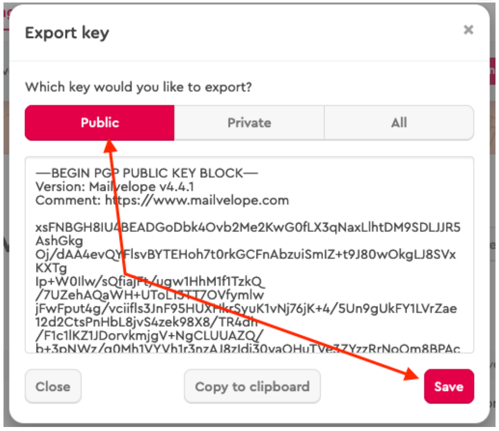
Primary	Name	Email	Status	Key server	Signatures
✓	Matthew R. Kisow	[redacted]@gmail.com	● valid	● synchronized	1

The key data on the Mailvelope key server is up to date.

Key details

Status	● valid	Key ID	8BBB2D7EECFE30C6
Created	02/03/2022	Algorithm	RSA (Encrypt or Sign)
Expires	never	Length	4096
Password	••••••••	PGP Fingerprint	7F4B 64A0 64AE ABE1 C794 FE95 8BBB 2D7E ECFE 30C6

10. On the Export Key screen, ensure "Public" is selected and click the "Save" button. Then click the "Close" button. This will save your Public-Key to your downloads folder with the name of <key name>_pub.asc.

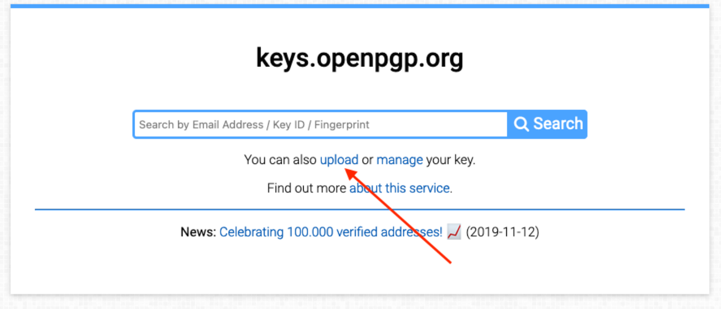


Which key would you like to export?

```
—BEGIN PGP PUBLIC KEY BLOCK—
Version: Mailvelope v4.4.1
Comment: https://www.mailvelope.com

xsFNBGH8IU4BEADGoDbk4Ovb2Me2KwG0fLX3qNaxLlhtDM9SDLJJR5
AshGkg
Oj/dAA4evQYFlsvBYTEHoh7t0rkGCFnAbzuiSmIZ+t9J80wOkgLJ8SVx
KXTg
Ip+W0Ilw/sQfiajFt/ugw1HhM1f1TzkQ_
/7UZehAQaWH+UToL15TT7OVfymlw
jFwFput4g/vciifls3JnF95HUXHkrSyuK1vNj76jK+4/5Un9gUkFY1LVrZae
12d2CtsPnHbL8jvS4zek98X8/TR4dh
/F1c1lKZ1JDorvkmjgV+NgCLUUAZQ/
b+3pNWz/g0Mh1VYVh1r3nzAJ8zIdi30vaQHuTVe3ZYzzRrNoOm8BPAc
```

11. Open a new Firefox tab and go to https://keys.openpgp.org. Then find and click on the upload hyperlink.

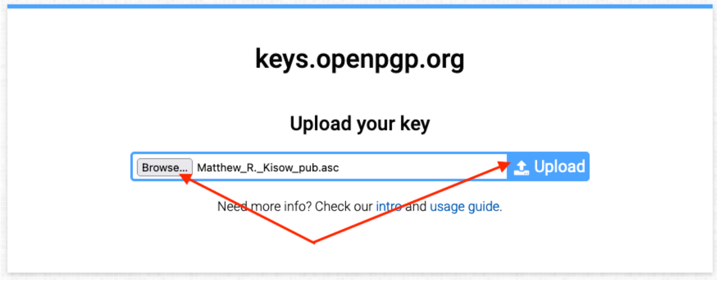


You can also upload or manage your key.

Find out more about this service.

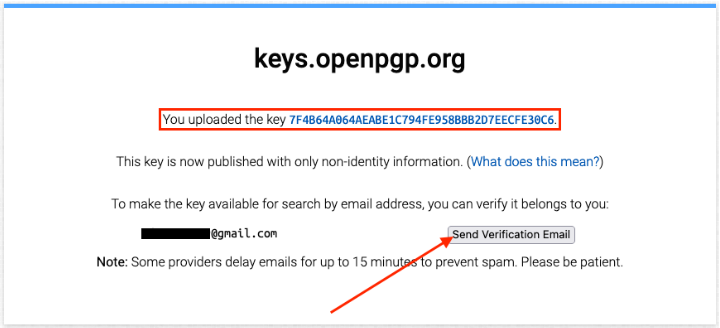
News: Celebrating 100.000 verified addresses! (2019-11-12)

12. From the "Upload your key" screen on *keys.openpgp.org*, select the Public-Key you exported in step ten and click the upload button.



Need more info? Check our intro and usage guide.

13. You will receive notification that a key with the cryptographic fingerprint was uploaded to the key server. To make this key searchable by your identified e-mail address, click the “Send Verification Email” button.



keys.openpgp.org

You uploaded the key 7F4B64A064AEABE1C794FE958BBB2D7EECFE30C6.

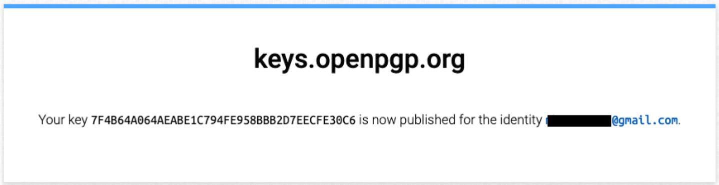
This key is now published with only non-identity information. (What does this mean?)

To make the key available for search by email address, you can verify it belongs to you:

[redacted]@gmail.com

Note: Some providers delay emails for up to 15 minutes to prevent spam. Please be patient.

14. Click the verification hyperlink sent to your e-mail address, to receive a confirmation message that your key has been published with your e-mail address.



keys.openpgp.org

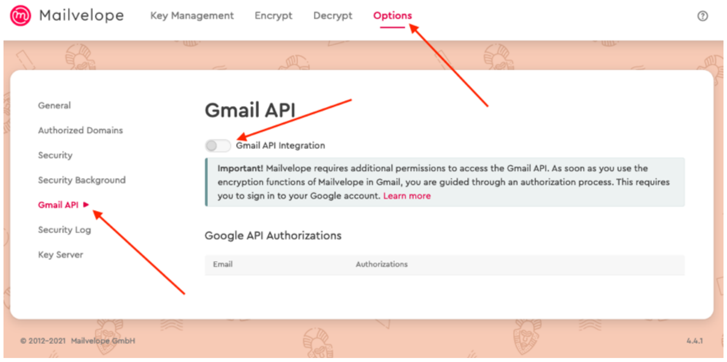
Your key 7F4B64A064AEABE1C794FE958BBB2D7EECFE30C6 is now published for the identity [redacted]@gmail.com.

15. To make a backup of your public/private key pair, repeat steps nine – ten selecting “All” followed by the “Save” button. This will save your public/private key pair to your downloads folder. Keep this key pair in a safe place.

2.3 Task 3: Sending An Encrypted E-Mail

In this task, you are going to search for your instructor's Public-Key on one of the two key servers that were used in this lab. Then you will send them an encrypted e-mail. You will collect your instructor's response and include it in your lab report.

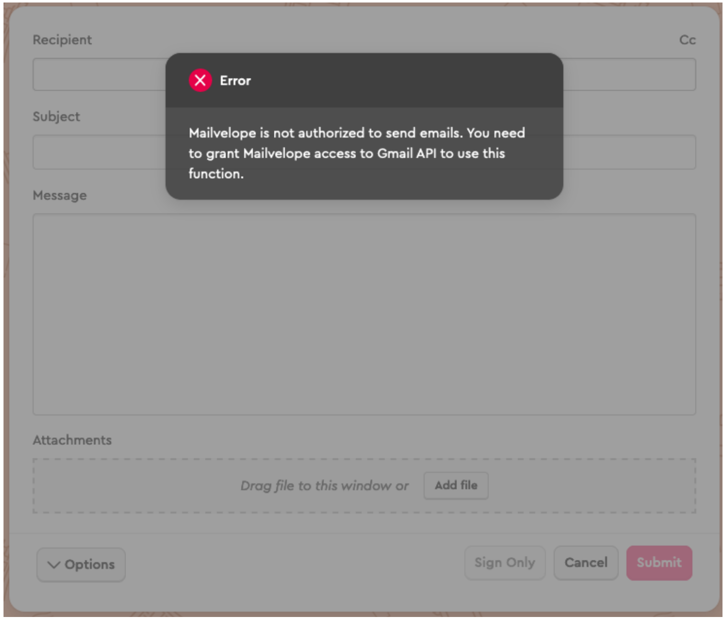
1. Click on the "Options" tab in Mailvelope. Then select the "Gmail API" located on the left of the screen. Click the slider-switch to enable "Gmail API Integration".



Important! Mailvelope requires additional permissions to access the Gmail API. As soon as you use the encryption functions of Mailvelope in Gmail, you are guided through an authorization process. This requires you to sign in to your Google account. Learn more

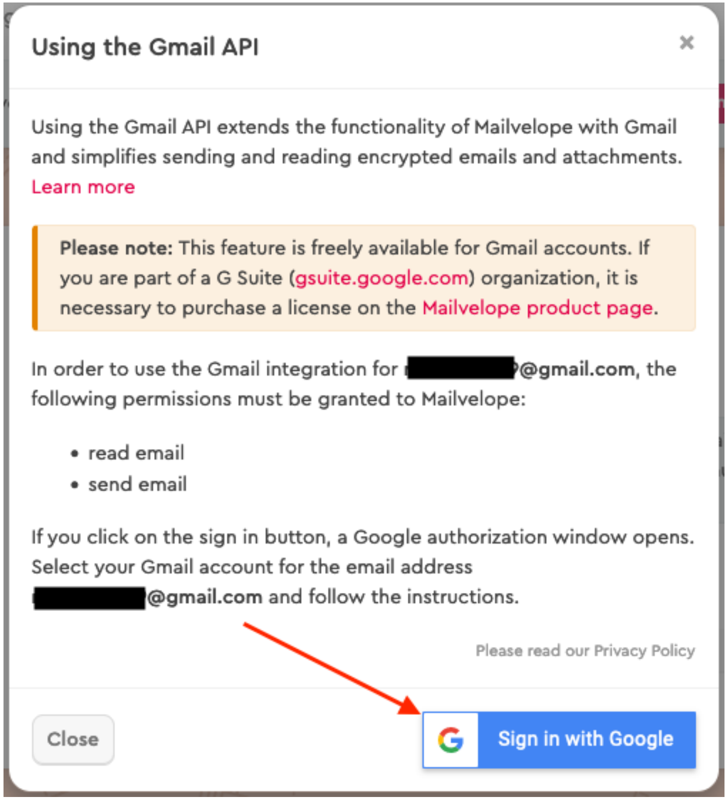
2. Return to your G-Mail inbox, and click the Mailvelope icon located on the left above your inbox.

3. When you click the Mailvelope icon in G-Mail, you will receive an error screen in a pop-up window.



Mailvelope is not authorized to send emails. You need to grant Mailvelope access to Gmail API to use this function.

4. On the "Key Management" screen in Mailvelope, in the "Using the Gmail API" window, authorize the use of the API by clicking the "Sign in With Google" button.



Using the Gmail API

Using the Gmail API extends the functionality of Mailvelope with Gmail and simplifies sending and reading encrypted emails and attachments. Learn more

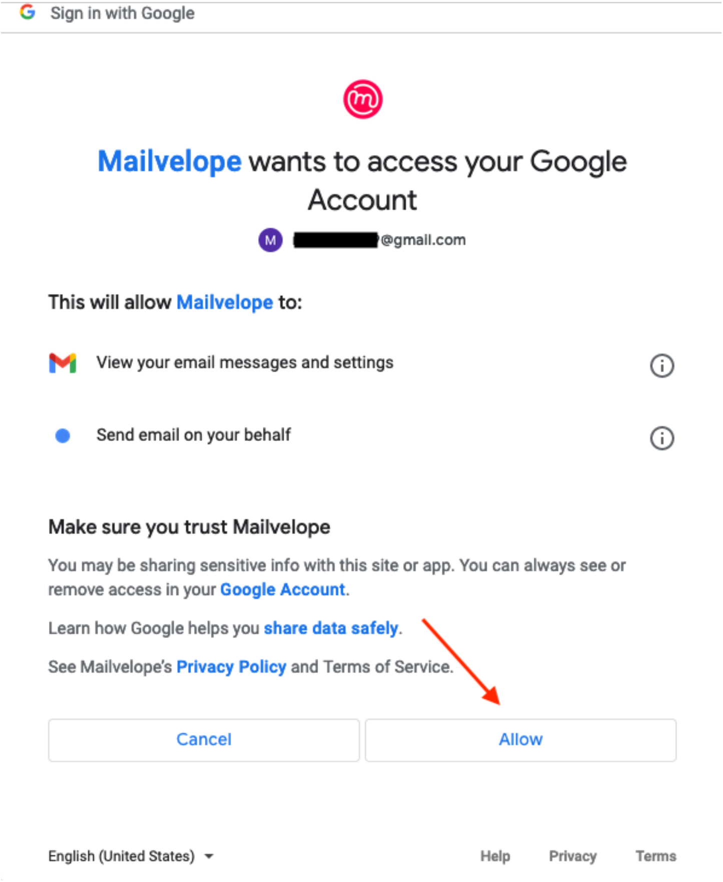
Please note: This feature is freely available for Gmail accounts. If you are part of a G Suite (gsuite.google.com) organization, it is necessary to purchase a license on the Mailvelope product page.

In order to use the Gmail integration for [redacted]@gmail.com, the following permissions must be granted to Mailvelope:

- read email
- send email

If you click on the sign in button, a Google authorization window opens. Select your Gmail account for the email address [redacted]@gmail.com and follow the instructions.

5. After providing your G-Mail credentials, click the “Allow” button to permit Mailvelope access to your G-Mail account. For now, you can close the “Mailvelope – Compose Secure Email” pop-up window.



Mailvelope wants to access your Google Account

M [redacted]@gmail.com

This will allow Mailvelope to:

View your email messages and settings

Send email on your behalf

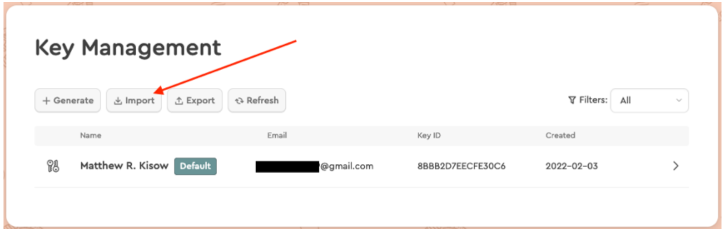
Make sure you trust Mailvelope

You may be sharing sensitive info with this site or app. You can always see or remove access in your Google Account.

Learn how Google helps you share data safely.

See Mailvelope's Privacy Policy and Terms of Service.

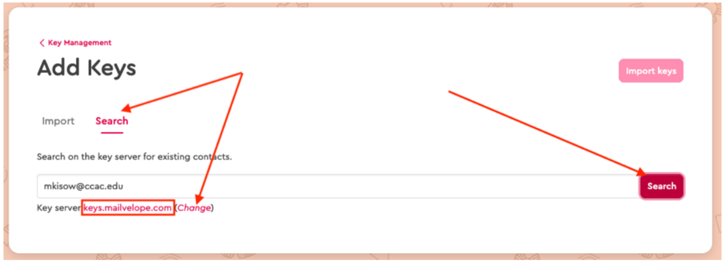
6. On the “Key Management” screen in Mailvelope, click on the “Import” button.



Key Management

Name	Email	Key ID	Created
Matthew R. Kisow Default	[redacted]@gmail.com	8BBB2D7EECFE30C6	2022-02-03

7. On the “Add Keys” screen in Mailvelope, click the “Search” tab. Then verify that the “Key server” listed under the search box defaults to *keys.mailvelope.com*[4]. In the search box, type in your instructor’s e-mail address, then click the “Search” button.



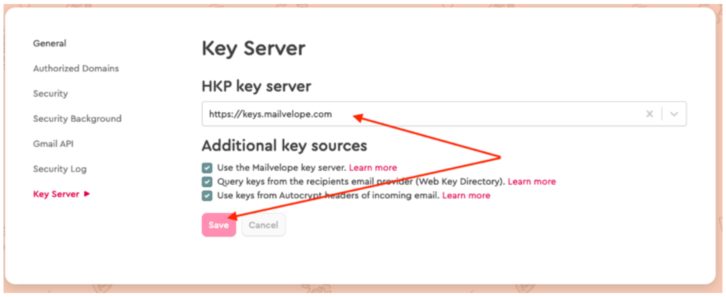
Search on the key server for existing contacts.

mkisow@ccac.edu

Key server keys.mailvelope.com (*Change*)

[4] *If the key server has not defaulted to keys.mailvelope.com, click the “Change” hyperlink and follow the instructions below to change it to the proper key server.*

From the “HPK key server” drop-down list, find and select *keys.mailvelope.com*, then click the “Save” button. Once the key server has been updated, return to step two above.



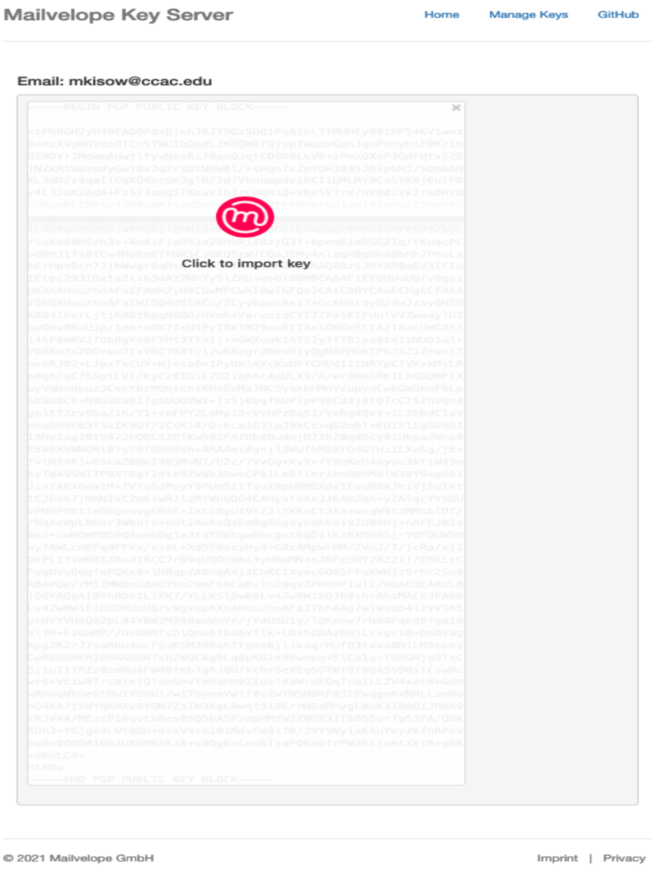
HKP key server

https://keys.mailvelope.com

Additional key sources

☑ Use the Mailvelope key server. Learn more
☑ Query keys from the recipients email provider (Web Key Directory). Learn more
☑ Use keys from Autocrypt headers of incoming email. Learn more

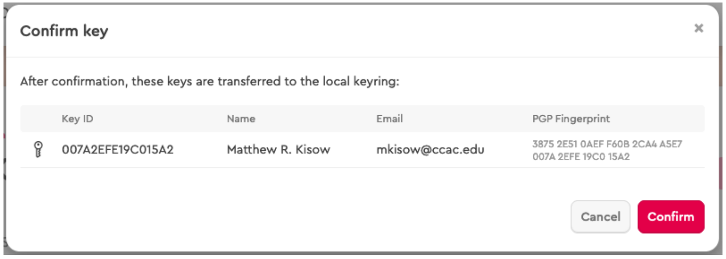
8. If the search is successful a new web browser tab "Mailvelope Key Server" will open. Click the key to import it into the Mailvelope keyring.



Email: mkisow@ccac.edu

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
[illegible]
-----END PGP PUBLIC KEY BLOCK-----
```

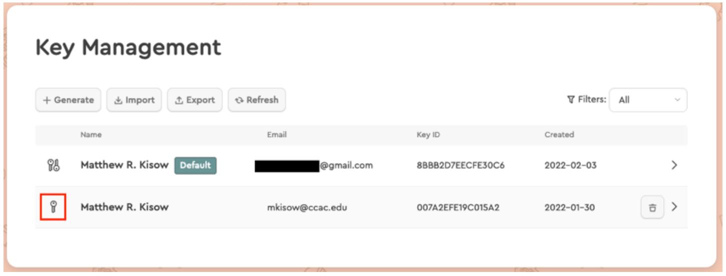
9. On the "Confirm Key" screen, click the "Confirm" button to finish importing your instructor's Public-Key.



After confirmation, these keys are transferred to the local keyring:

	Key ID	Name	Email	PGP Fingerprint
	007A2EFE19C015A2	Matthew R. Kisow	mkisow@ccac.edu	3875 2E51 0AEF F60B 2CA4 A5E7 007A 2EFE 19C0 15A2

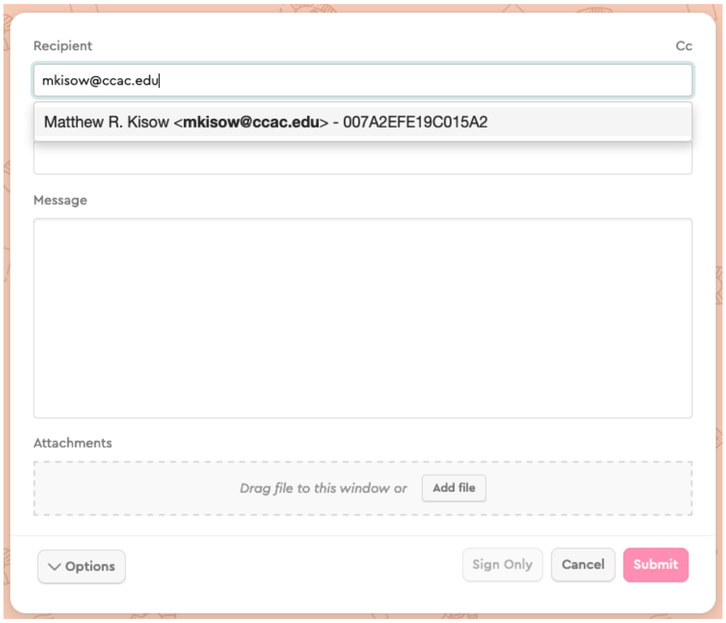
10. After the key import, you will be returned to the "Key Management" screen in Mailvelope. Your instructor Public-Key will be displayed, note the icon indicating this is only one key in the key pair.



Key Management

	Name	Email	Key ID	Created
	Matthew R. Kisow Default	[redacted]@gmail.com	8BBB2D7EECFE30C6	2022-02-03
	Matthew R. Kisow	mkisow@ccac.edu	007A2EFE19C015A2	2022-01-30

11. Return to your G-Mail inbox and click the Mailvelope icon. The "Mailvelope – Compose Secure Email" pop-up window will open. In the recipient box type your instructor's e-mail address, a completion box should appear with their Public-Key ID.



Recipient

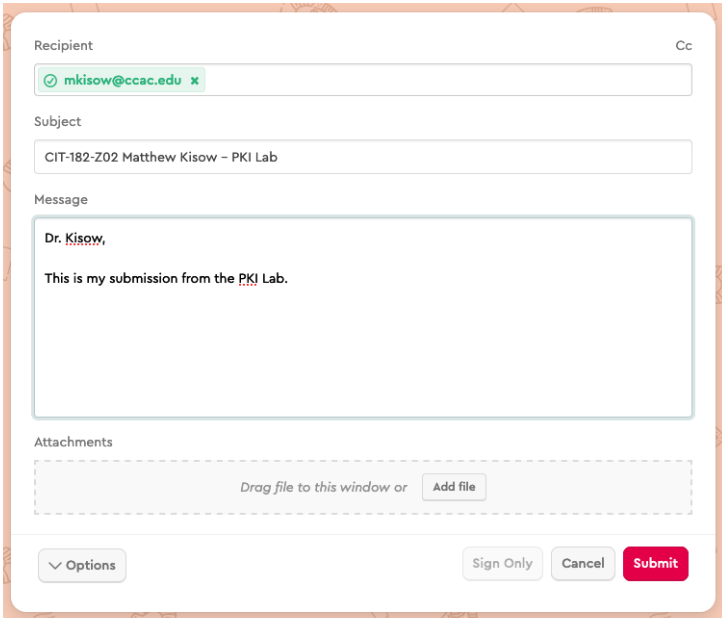
mkisow@ccac.edu

Matthew R. Kisow <**mkisow@ccac.edu**> - 007A2EFE19C015A2

Message

Attachments

12. Compose your message per your instructor's requirements, then click the "Submit" button. You will receive an encrypted reply from your instructor.



Recipient: mkisow@ccac.edu

Subject: CIT-182-Z02 Matthew Kisow – PKI Lab

Message:

Dr. Kisow,

This is my submission from the PKI Lab.

3. Submission

You need to submit a detailed lab report with screenshots that describe what you have done and what you have observed. You will also need to provide a narrative that explains your observations, particularly anything that you found interesting or surprising.

At a minimum your lab report must include:

- A cover page.
- A summary paragraph that describes your experience using PKI.
- A narrative of your observations, noting any findings you found interesting or surprising.
- A screenshot of your public/private keypair from the Mailvelope Key Management tab.
- Screenshots from *keys.mailvelope.com* and *keys.openpgp.com* that show your Public-Key's listed on these two (2) key servers.
- A redacted screenshot of the backup of your public/private key pair.
- A copy of the decrypted e-mail that your instructor sent you.

This report should be written in Microsoft Word. The title page should include the name of the lab, your name, class number and section and, the date.

Send your lab report in an encrypted e-mail to your instructor.

Rubric

X	POINTS	REQUIREMENT OR LEARNING OBJECTIVE
	5	Cover Page
	20	Summary paragraph that describes students experience using PKI
	20	Narrative of the students observations and findings
	5	Screenshot of the students public/private key pair
	5	Screenshots from the two public key servers
	5	Screenshot of the backup of the students redacted public/private key pair
	10	A copy or screenshot of the decrypted e-mail that was sent from the instructor to the student.
	5	The lab report was written in Microsoft Word or equivalent format
	5	The lab report title page has all requested information
	10	There are no spelling or grammatical issues
	10	The report was sent to the instructor in an encrypted e-mail.