

# Secure eMails with Mailvelope

## 1. Introduction

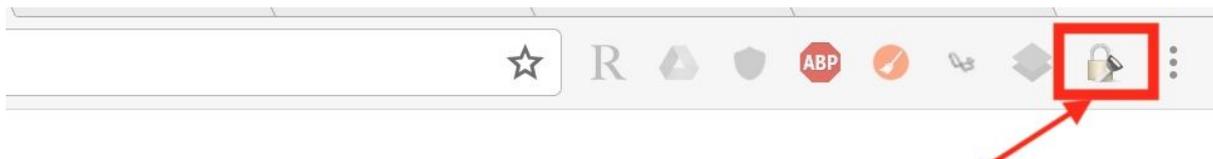
Mailvelope is a browser add-on or a plugin that extends its capability in encrypting email contents and is based on OpenPGP cryptography standards. To be able to send, receive or digitally sign emails securely using OpenPGP based services like Mailvelope, users first have to create public, private key pair and share the public key.

## 2. Installation

Click the following links to install Mailvelope on Google Chrome and Firefox browsers:

- Google Chrome  
<https://chrome.google.com/webstore>.
- Firefox
- [download.mailvelope.com](https://download.mailvelope.com)

If Mailvelope is successfully installed, a lock icon is displayed somewhere in the main toolbar, beside the address bar as shown in the image below.



Click this icon to configure your encryption keys and access other management settings.

## 3. Basics

To be able to encrypt emails you need to:

- a. **Generate** encryption keys (*Public and Private key pair*) to **receive/sign** encrypted emails
  - i. Public key – It is a key used for encrypting a message. The key must be made available to the public. It is mainly used while sending an encrypted email. When you send an encrypted email, you will need to use the public key of the recipient.
  - ii. Private key – Used to decrypt a message. To decipher or read an encrypted message, you need to use the private key. This key should

be kept away from anyone else who is not its owner. Needs to be stored securely. Access is restricted by password.

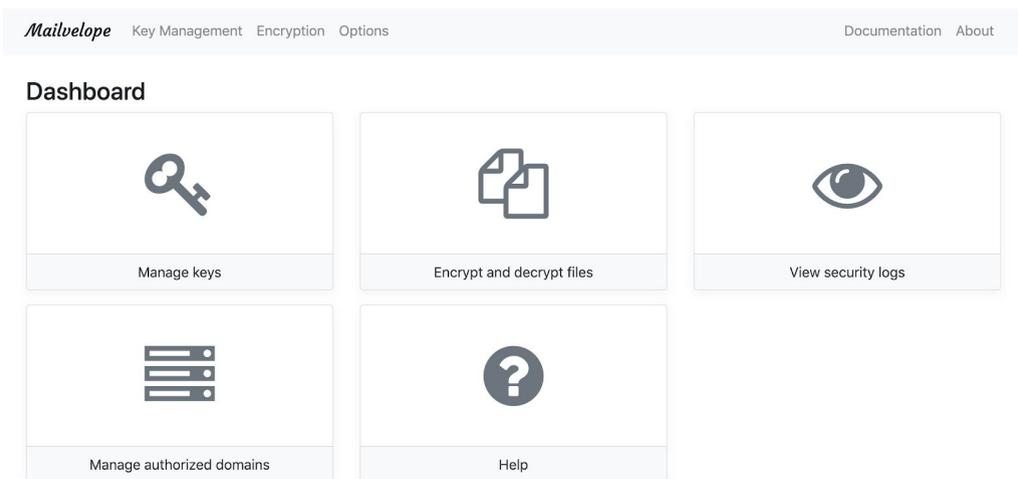
- b. **Import** public keys of users you want to **send** encrypted emails to

This concept is illustrated on the page "[How Gpg4win works](#)". Gpg4win is another application based on the same working principles.

## 4. Key Management

Before we go on to encrypting emails , let's see how we handle keys for that.

Click on Mailvelope's lock icon  in the toolbar and click on dashboard, you will land in the following page. From here click on manage keys



## 5. Generating Keys

Click **Generate +** to open the key generation dialog. Fill out the boxes and assign a key password. Make sure you never lose this password. If it is lost, the password cannot be recovered and the key can no longer be used. It might be a good idea to use your **keychain Access/keepass** (Password Manager) to manage your newly created password.

Enter all the necessary information, click on advance and ensure secure algorithm and key size is selected . Click **Generate** to start generating a key. Repeat for any other email accounts.

**Mailvelope** Key Management Encryption Options Documentation About

### Generate Key

Name  
test

Full name of the key owner

Email  
test@test.org

<< Advanced

Algorithm  
RSA

Key size (Bit)  
4096 Bit

Key expiration date  
04/26/2020

Enter Password  
\*\*\*\*

Re-enter Password  
\*\*\*\*

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

Generate Back

Afterwards, you can see the result in the key list by selecting **Key Management**.

**Mailvelope** Key Management Encryption Options Documentation About

### Key Management

Generate Import Export Refresh Filters: All

Name	Email	Key ID	Created
test <b>Default</b>	test@test.org	52FE1E4E8AE16B23	2019-05-22

## 6. Importing Keys

To import existing keys, click **Key Management** in the option menu and then **Import Key**. You can import key either from public key servers, from a text file or paste text. Following demonstrated importing key from key server.

**Mailvelope** Key Management Encryption Options Documentation About

### Key Management

#### Import Keys

Key search  
Search for public keys on key server.  
info@eff.org Search

Key server [keyserver.ubuntu.com](#) (Change)

Import key from file  
Select a key text file to import

Import key as text  
Please insert one or multiple keys in text format here.

Import Back

Search results will be displayed on the key server website in a new tab.

## Search results for 'org info eff'

Type	bits/keyID	Date	User ID
pub	2048R/ <a href="#">4B18732F</a>	2013-01-12	<a href="#">EFF Info</a> < <a href="mailto:info@eff.org">info@eff.org</a> >

After clicking on the displayed **keyID**, the key text will be shown and Mailvelope will be able to detect the key.

### Public Key Server -- Get "0x11a1a9c84b18732f "

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.6
Comment: Hostname: keyserver.ubuntu.com

mQENBFDwfsBCADr1/u4x1RNuYiG1YJicGVg2d0erxp+t0mNF7VV5accY44L7JCO+Y6Zcatv
rm6d/ARQ7fEv32v0ILmulh6xwVum92zUaTl2Ql5JLEN9k4zB1I9LS1LXoRvH1SKFhx+GYr+yyq
b2Eull11515UKTGMERT9tPv1/ObnAG1z5u6JWFTTlDa01zsjYXm8e74HQfU/3pM5Ebp4GGRi
Eh319RkmskuGfE8E3asW1jQc0cFp40f+kCQD0HLe62QXsWm11bbTSL049QpF7E54T9A
MKGBe9SaY8RQxB19tIRi4tWz0K5ygmQPOJARGzRftrXKlpi10j2A/6Vof+2ucru9hABEB
AAG0F0VGRiBjbmZvIDxpmbzVqCvMzI5vcmc+1EYEEBCAAyFAl16iKUDAcgQU15UaPAPoWKL
pgCeKZyPftessF+GBRzfHtqEqAB4YAnRK3XNQCtHFG48BMAB1Eum9KrfktlEwEExECAAwfL
AlJKIzYFgw0rC4AACgkOrI3pBH2aFserhwCfWu8seN8DdFh/dswHum8ggw1zqVMAoKP4jOEt
uKz3SXdwbpj1Bc39EE7CiKAEBMKAAYFAlf1PaAcGkQMyZHVg8m4v2lMqIGPBT69AlBvEkc
7/kfWbmg/zCj8EoQHmb5rc9Sdu740g/Tzc++YyVFr2DzVG+OLW2NpOv1LXcLmqS0mKDLbW37X
RywCBjYzHtpL01Um+0XgB5aEJATpLzYyDpwrBIhmcG8Ykkl1k8cOpR4nnOJAoP0Ik3gmyDXn
c+cCSLqJmsDDy9RSpelSiQECCBABCAGBQJSSh8dAa0JEJlq3zr0zvClxVgH/3ED10r4MIIM
cUx6uvHGPb0q04My2uVzQAl80QgYJzyNE2JqfWUu+/IGWN+QK5JjrLDpT4CfICyjbY/Q+J8
FsykuYLEGbTTRCACmcbp3VA9HW0YnV881JzWjWfSnRj8+44+XMcC4ItBLVX9Nhb6p21mFn
E1Tnd0BQ0Dnrqyffbba3cxelSDIx+niyKdal/cQNg6cpu1A+HmzMDpri4xjyvAyEUzmpNOL
sivAEQFKY8nQh8Rm5e512nLcseH8KudZn7R1DGHYni7dJpk4BBaifAwwXpUnidvu/aLqDI
LlFz18zMF1R0TcsbBehkjcNbx6Prr7YRzENfA6QMY0yJARwEEAEIAAYFALcKc0IACgkQC9W3
HysGgTeRwI/SRHRcWuDDTR4PcxwZV18cYnMCgjqB0F1K21S31uXb5w3r1G1v+1PtZkdyV0
```



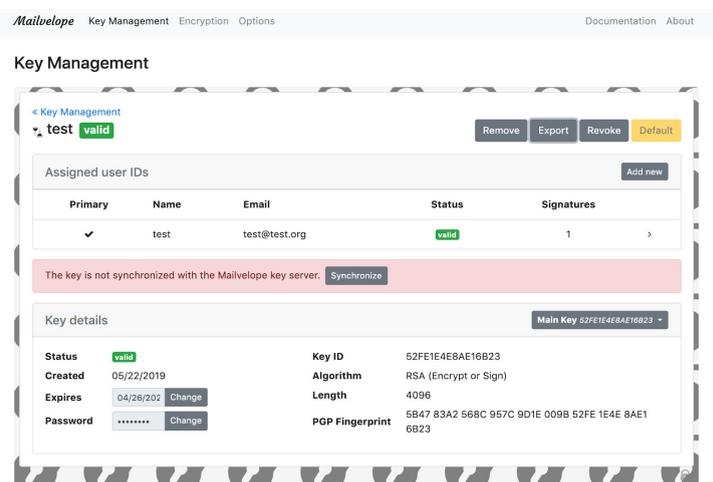
With another click on the key symbol the key is imported into Mailvelope.

## 7. Exporting Keys

Key export functionality is used to export keys into ``.asc`` files or to copy the file to clipboard. We can use this function to make public keys available for others to import or to make a backup of a public-private key pair in a secure place.

To export all keys, click **Key Management** in the option menu and then **Export Key**.

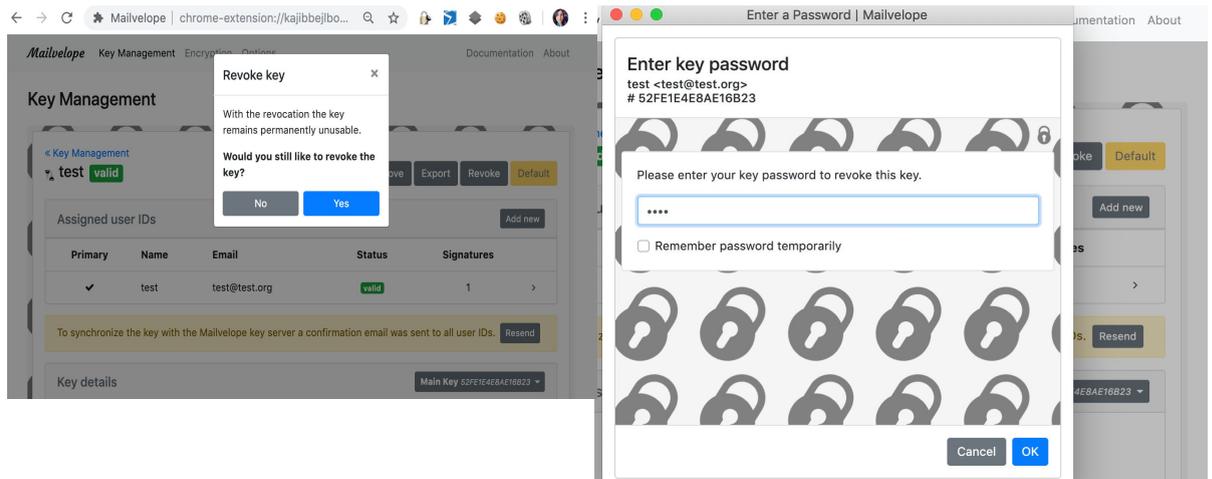
To export individual key, click **Key Management** in the option menu, select the key and then **Export**



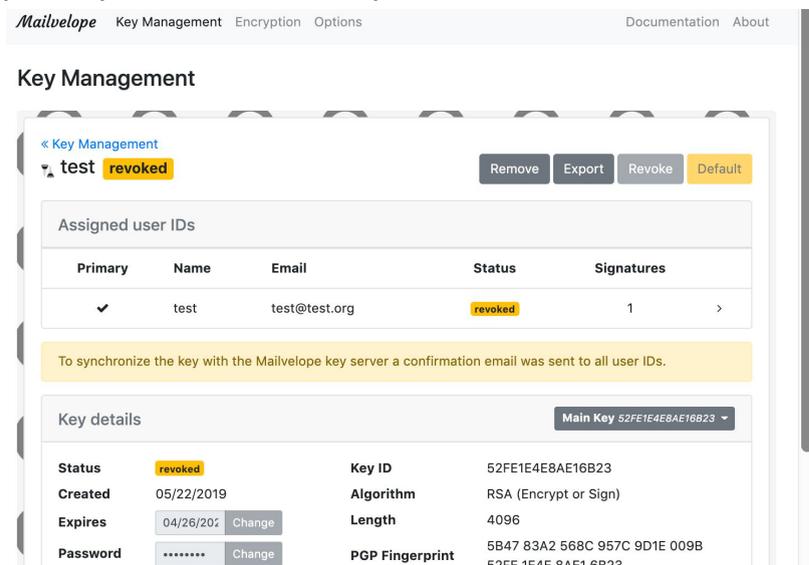
## 8. Revoke Keys

To revoke keys/ delete them from mailvelope server, click **Key Management** in the option menu, select the key and then **Revoke**.

You can also delete it from <https://keys.mailvelope.com/manage.html>



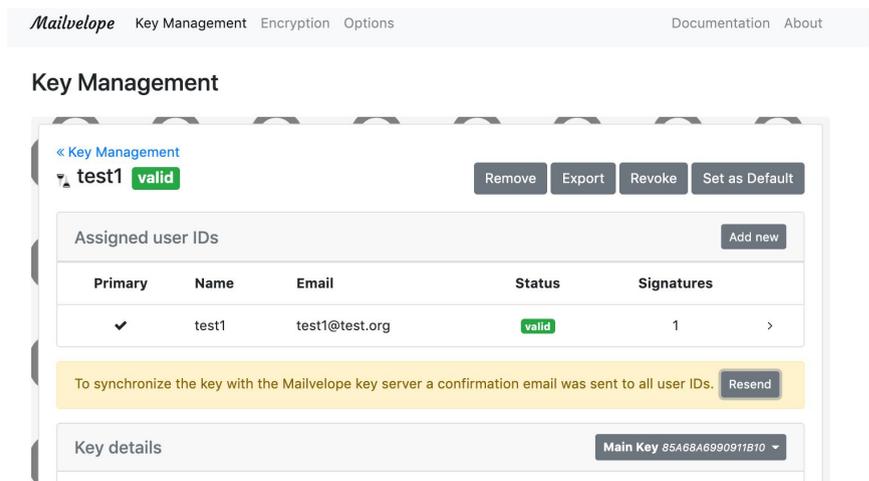
If the email id exists and the operation has been successful your key status will change to Revoked. Confirmation link will be sent to your email, once you confirm, your key is removed from key server.



Check your inbox for new email from Mailvelope and follow the instructions there to complete key removal.

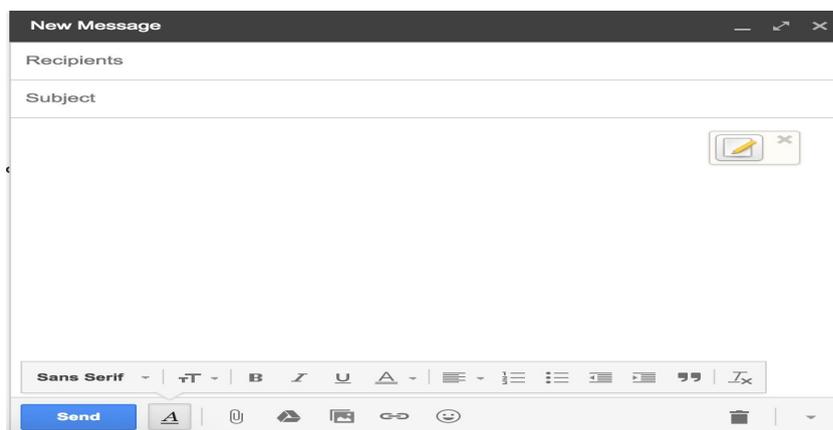
## 9. Defining the primary Key

To define a key as primary/default key them, click **Key Management** in the option menu, select the key click and then **Set as Default**. The primary/default key is always used unless another key is explicitly selected.

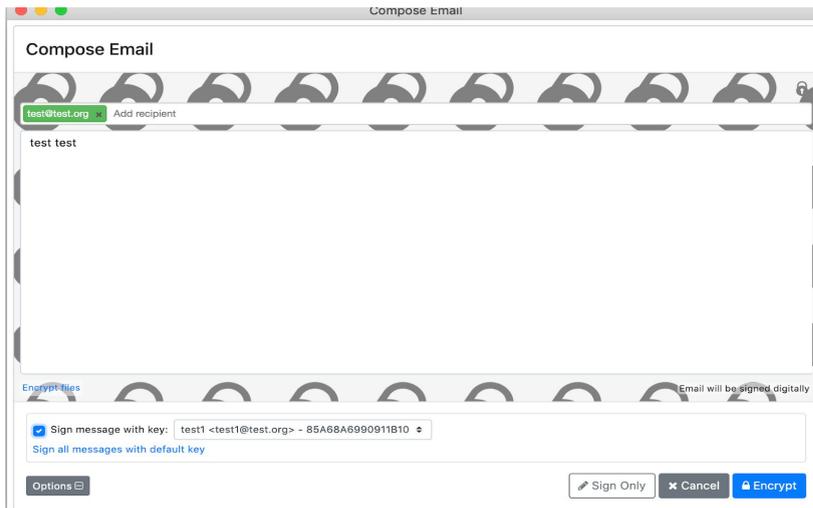


## 10. Encrypting Messages

Email messages are created and encrypted in an external editor. The compose button  is displayed in all email composing areas of the webmail provider and will launch Mailvelope's external editor.



Clicking on the **Compose** button will open a new popup with a separate editor. This ensures that the email creation and encryption process is completely isolated from the webmail provider.



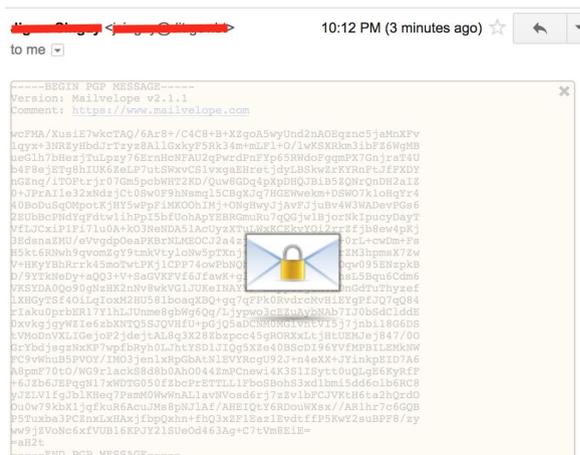
The email can now be composed. You can choose the recipients, or more specifically the people who should be allowed to decrypt the message, by adding the email address to the upper input field in the dialog. Like in other email clients you can also search in this field for recipients by name. For each recipient, there has to be a public key available in Mailvelope's keyring. If you enter an unknown email address, Mailvelope will automatically search the Mailvelope key server ([keys.mailvelope.com](https://keys.mailvelope.com)) for PGP keys and import the matching keys without further action required. Alternatively, you can also import keys manually as described in [Importing keys](#) earlier.

Next, click the **Encrypt** button to encrypt the message and transfer the results back to the webmail client

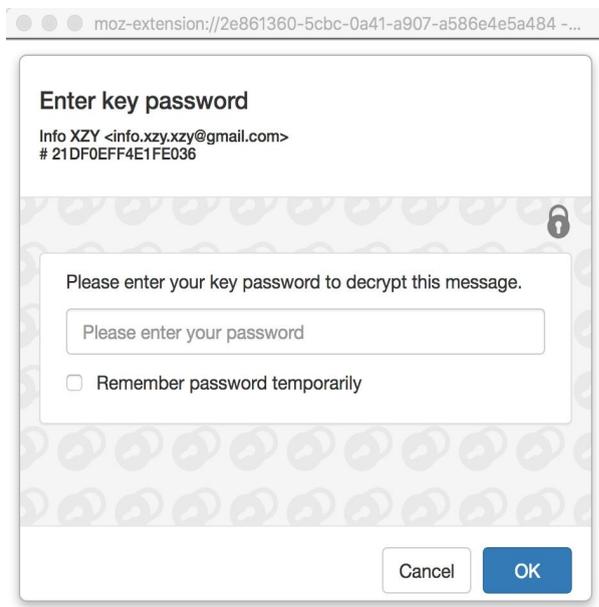
With the **Options** button in the Mailvelope editor you can access the option to sign the message.

## 11. Message Decryption

Whenever Mailvelope detects an encrypted message in your webmail client, it marks the mail with a closed envelope icon. Click on it to decrypt the message.



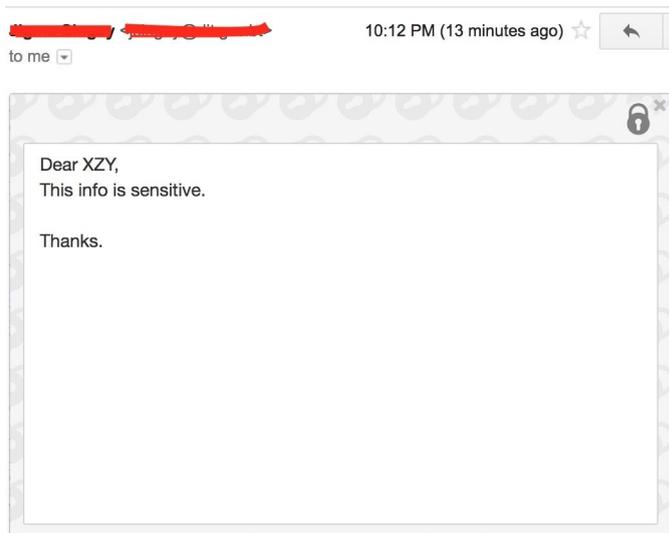
Next, enter your key password and click **OK**.



Mailvelope tries to find the private key that is required to decrypt the message. If the correct key is found in the keyring, the corresponding User and Key ID are displayed in the password dialog.

If Mailvelope does not have the correct private key to decrypt the message in its keyring, the following error message is displayed: **No private key found for this message. Required private key IDs: ....**

After the key is unlocked with the password, the message is decrypted and directly shown in the marked area.



If an encrypted message contains a signature, Mailvelope will verify the signature and show the result with a label in the upper right corner of the decrypted message.

A click on the *Signed digitally* label will open up a dialog showing the verification result and signature details.

Signature verification is currently only enabled for the following email providers: Gmail™, Outlook.com™ and Yahoo!™.

## 12. File Encryption

Click on Mailvelope's lock icon  in the toolbar to open the main menu. Click **Options** and choose **File Encryption** from the top menu bar.

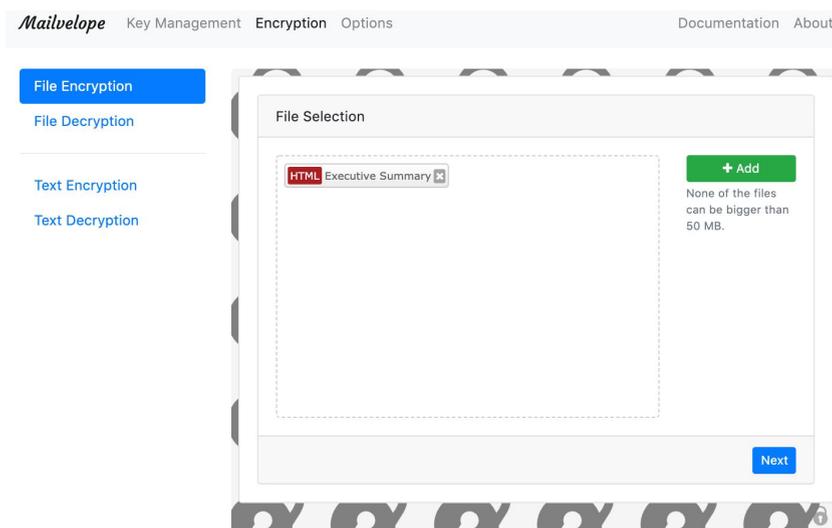
With the file encryption feature of Mailvelope, you can encrypt files on your storage devices according to the PGP standard. As with email encryption, the files will be encrypted with the recipient's public key.

The file encryption feature can also be used to encrypt and decrypt email attachments.

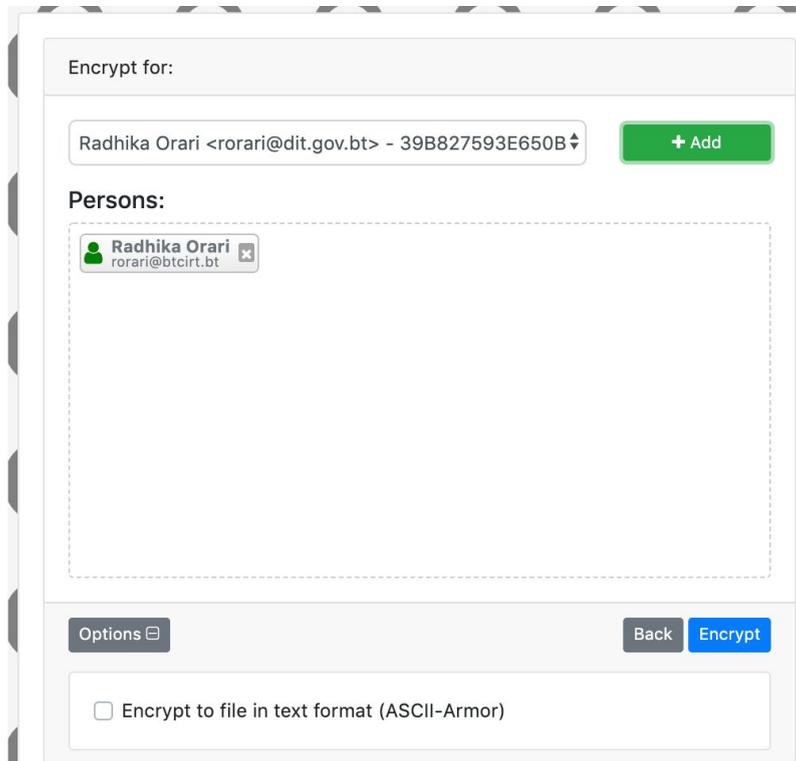
**Background:** email providers that directly integrate Mailvelope into their email application will support encrypted email attachments automatically. For email providers like Gmail™, Yahoo!™ or Outlook.com™ there are restrictions in the Mailvelope editor and encrypted attachments are not directly supported. The file encryption outlined here offers an alternative in this case, as it is possible to encrypt email attachments manually instead.

- Encrypt files

In a first step files on the storage devices will be selected for encryption with **Add**.

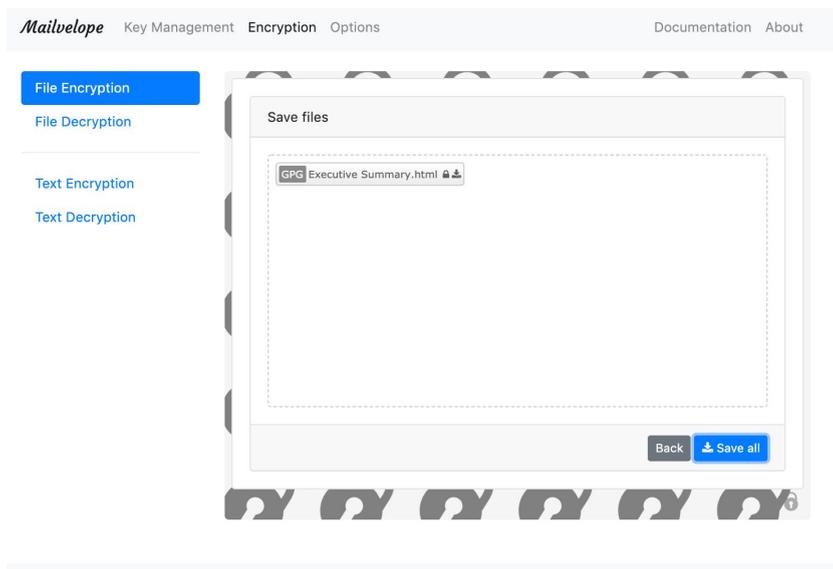


Click on **Next** and choose the recipients you want to encrypt the files for.



The screenshot shows a dialog box titled "Encrypt for:". At the top, there is a text input field containing "Radhika Orari <rorari@dit.gov.bt> - 39B827593E650B" and a green "+ Add" button. Below this is a section titled "Persons:" with a dashed border. Inside this section, there is a card for "Radhika Orari" with the email "rorari@btcirt.bt" and a close icon. At the bottom of the dialog, there is an "Options" button, a "Back" button, and an "Encrypt" button. Below the "Options" button, there is a checkbox labeled "Encrypt to file in text format (ASCII-Armor)".

The file by default will be saved as .gpg, you can click on option and check **Encrypt to file in text format(ASCII-Armor)** to save as .asc. After clicking **Encrypt** the files are encrypted for the selected recipients. Finally click on **Save all** to save the file



The screenshot shows the Mailvelope interface. The top navigation bar includes "Mailvelope", "Key Management", "Encryption", "Options", "Documentation", and "About". On the left, there is a sidebar with "File Encryption" (highlighted in blue), "File Decryption", "Text Encryption", and "Text Decryption". The main area shows a "Save files" dialog box with a dashed border. Inside, there is a card for "GPG Executive Summary.html" with a download icon. At the bottom of the dialog, there is a "Back" button and a "Save all" button.

- Decrypt files

The steps to decrypt files are similar to the encryption process. First, choose **File Decryption** in the left menu. Then, use the **+ Add** button to select the file to be decrypted. The decrypted files will be displayed once you enter your private key password.

