linuxbabe.com

How to Encrypt Emails with OpenPGP in Thunderbird (2022) - LinuxBabe

Xiao Guoan (Admin)

7-9 minutes

In previous parts of the GPG tutorial series, I explained how GPG encryption works. In this tutorial, you will learn how to **send encrypted emails in the Thunderbird email client**, so you don't have to type commands in the terminal. Thunderbird includes built-in OpenPGP support starting with version 78. It can encrypt your emails and also add digital signatures to your emails.

Step 1: Install Thunderbird

Windows and macOS users can download Thunderbird installer from the official website.

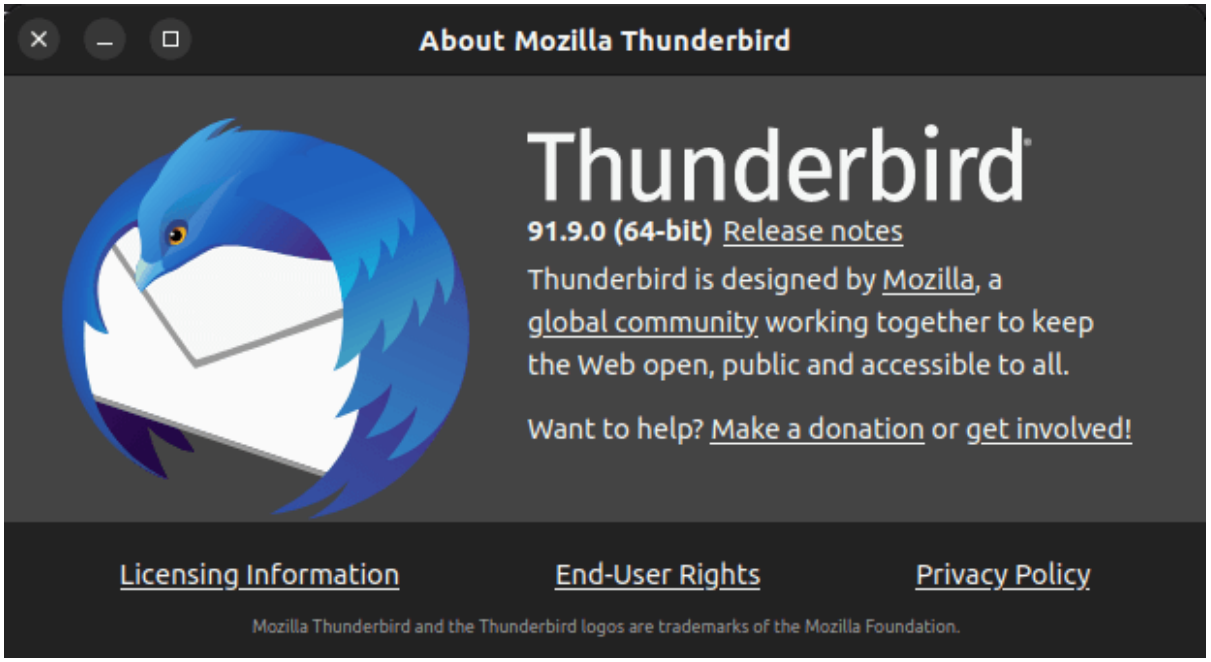
Linux users can install Thunderbird from the default software repository.

- Debian/Ubuntu: `sudo apt install thunderbird`
- CentOS/RHEL/Fedora: `sudo dnf install thunderbird`
- OpenSUSE: `sudo zypper install thunderbird`
- Arch Linux: `sudo pacman -S thunderbird`

Step 2: Check Your Thunderbird Version

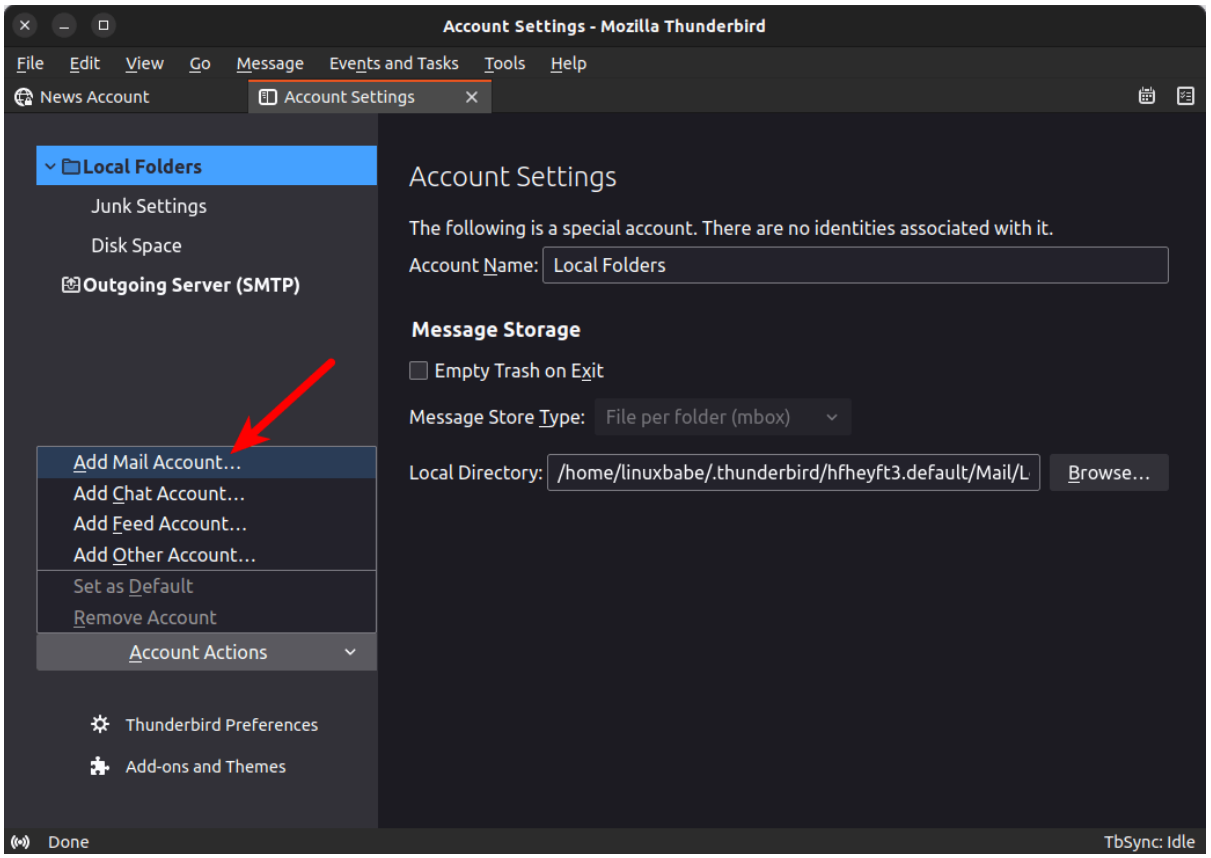
To use the built-in openPGP encryption, you need should be running Thunderbird v.78 or higher. To check the version number, go to the Thunderbird menu bar, select `Help` -> `About`

`Thunderbird`.



Step 3: Add Your Email Account in Thunderbird

Before using OpenPGP encryption, you need to add your email account in Thunderbird. Go to `Edit` -> `Account Settings` -> `Account Actions` -> `Add Mail Account` to add your email address in Thunderbird.



And verify you can send and receive emails in Thunderbird.

Step 4: Understand How OpenPGP Encryption Works

If you need to send an encrypted email to a recipient with OpenPGP, follow these steps

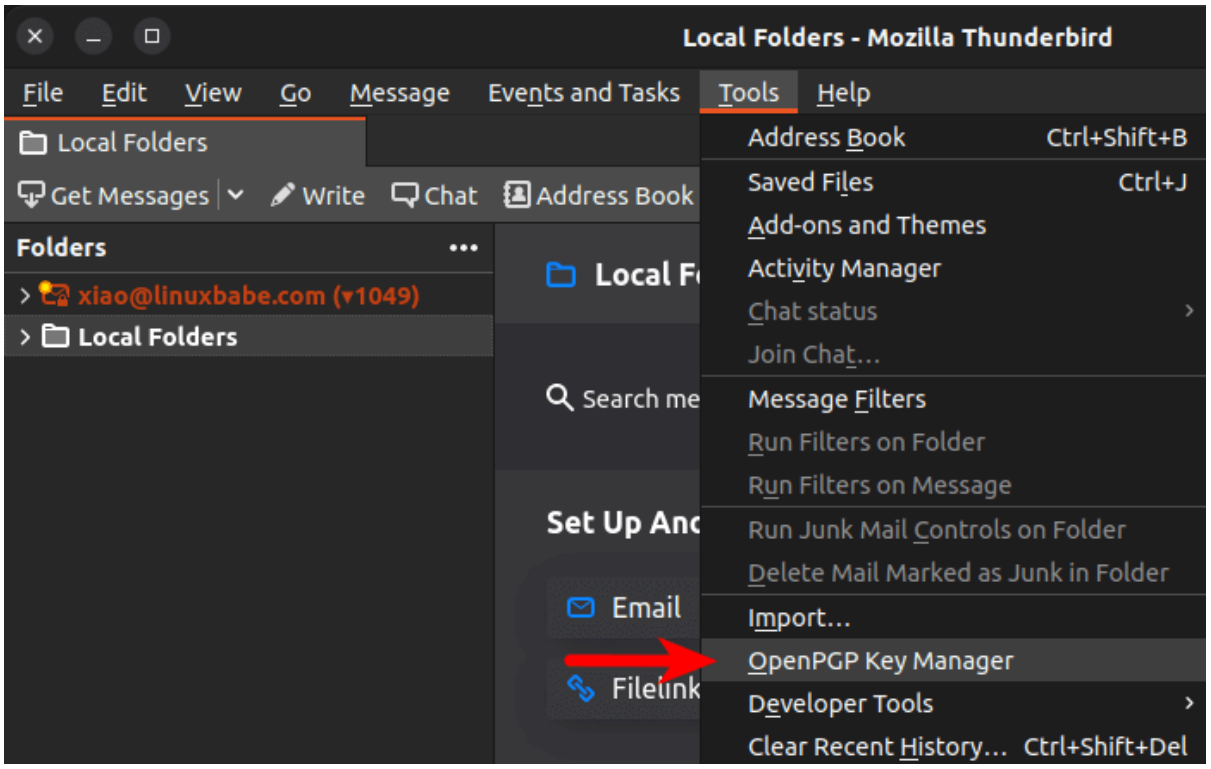
- Import the recipient's public key to your keyring.
- Encrypt the email with the recipient's public key
- Send the encrypted email to the recipient.
- The recipient decrypts the file with his/her own private key.

Step 5: Generate or Import GPG Key Pair

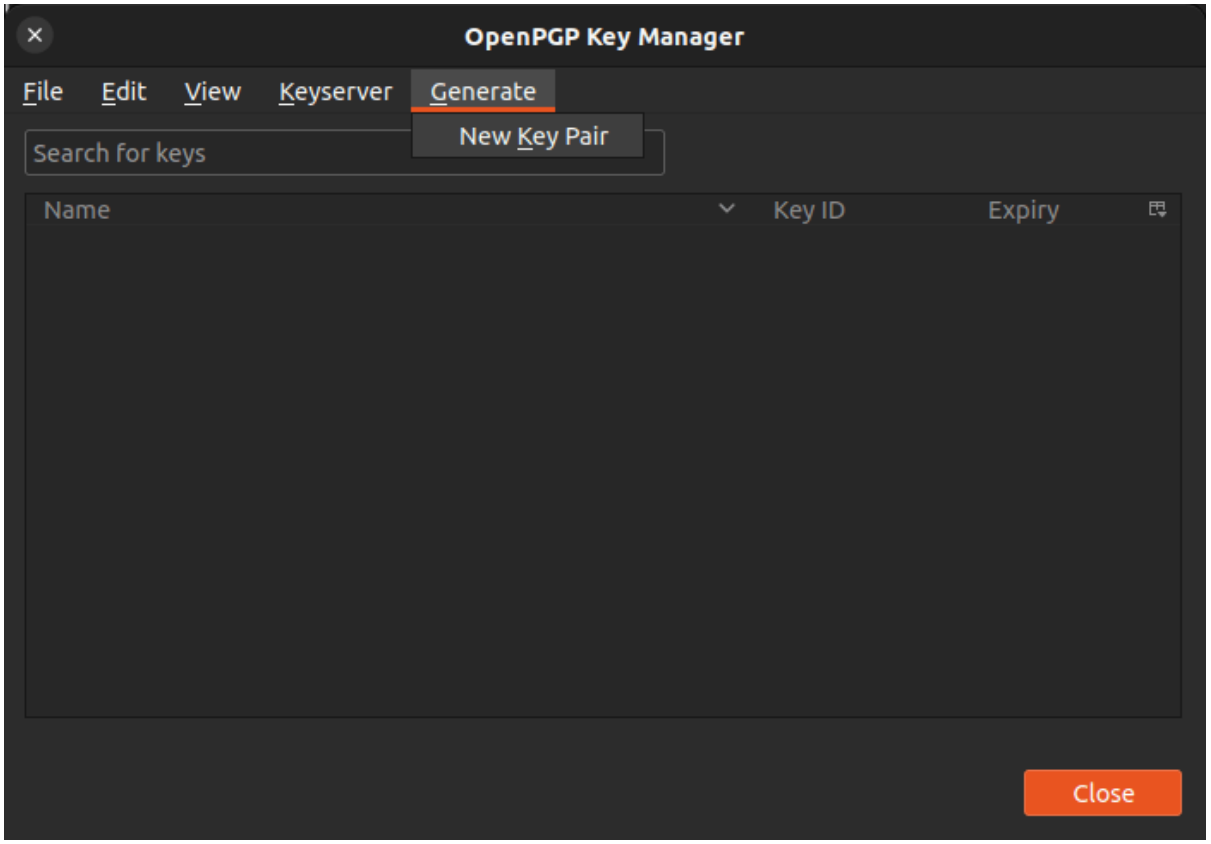
- If you don't have OpenPGP key pair, you can generate one right in Thunderbird.
- If you follow my previous GPG tutorial, then you should have a key pair managed by GnuPG. You need to import it to Thunderbird.

Generate a key pair

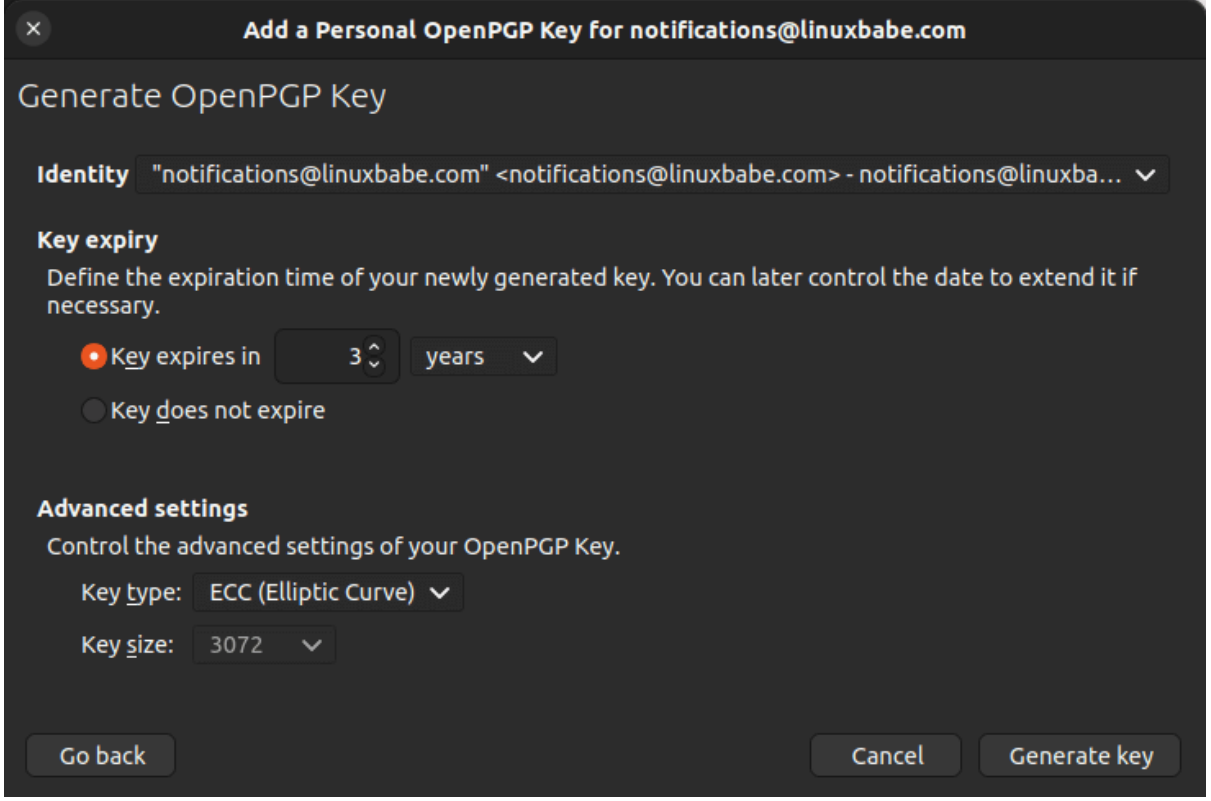
In the Thunderbird menu bar, select `Tools` -> `OpenPGP key manager`.



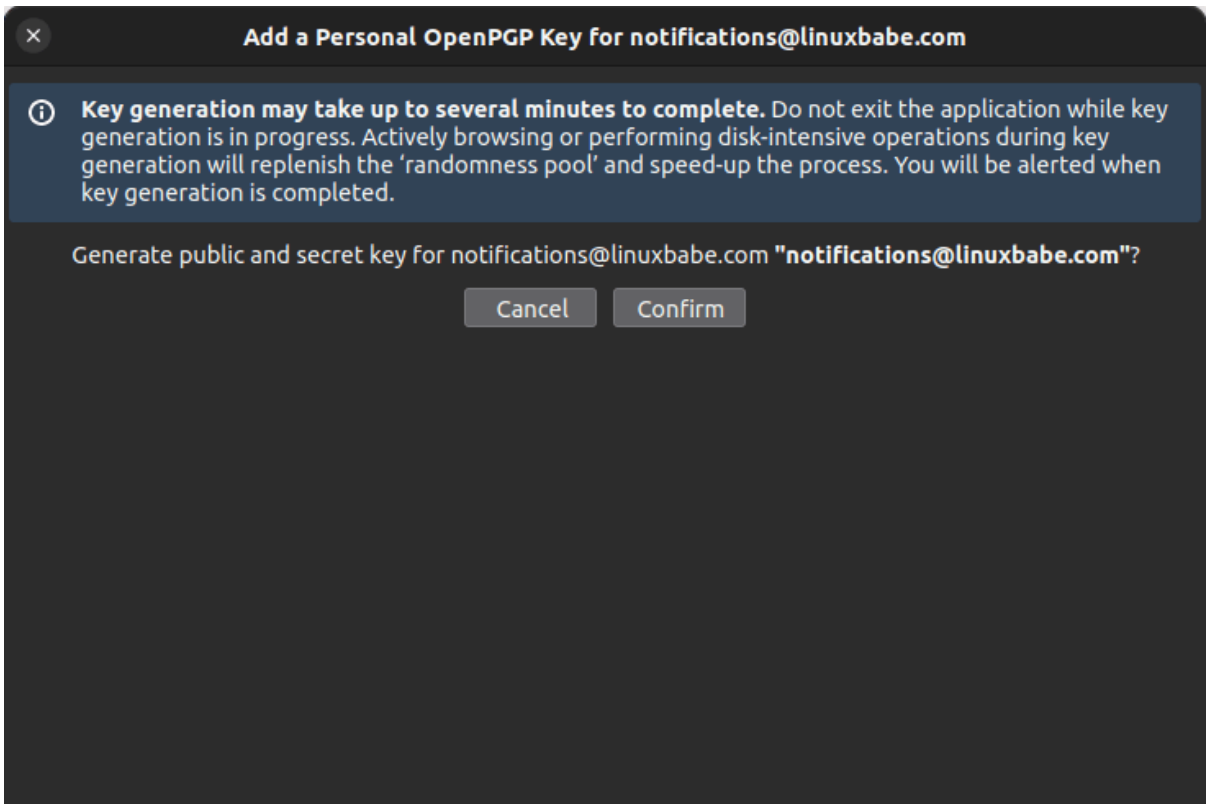
Then select **Generate** -> **New Key Pair**. (Note that if you didn't add an email account in Thunderbird, then you won't be able to generate a key pair in Thunderbird.)



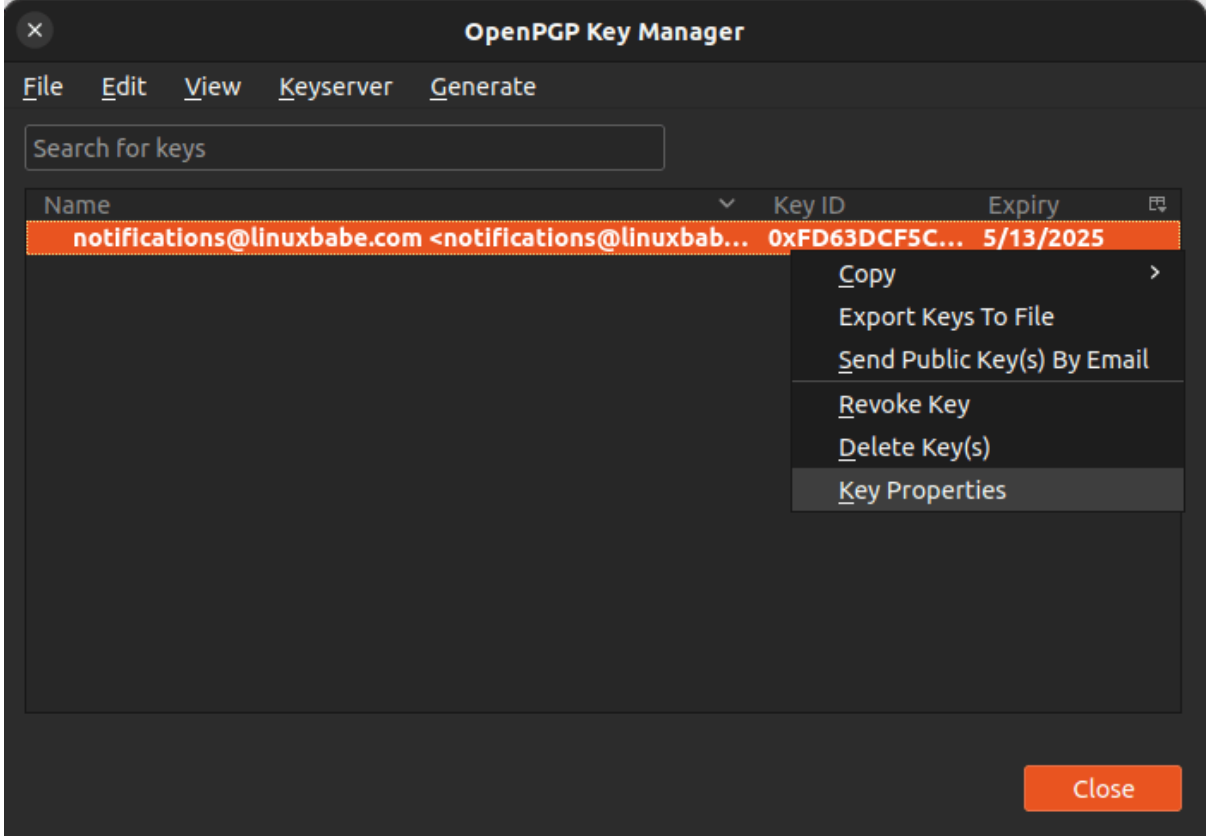
- If you have multiple email accounts in Thunderbird, then you can select an email address from the `Identify` dropdown menu. I have only one email account on this computer, so I use the default identity.
- Your key will expire in 3 years, which is fine. You can always extend the time in Thunderbird when your key is about to expire.
- By default, Thunderbird creates a 3072-bit RSA key, but ECC key is more secure, so select **ECC (Elliptic Curve)** as the key type.



Click **Generate Key** button. You will be asked to confirm you want to generate the key pair, click **Confirm** button.



Your key pair will be generated in a jiffy. It will appear in the OpenPGP key manager window. You can right-click on it and select **Key Properties** to check detailed information about your key. You are able to extend the expiration time in the **Key Properties** window.



Import your key pair

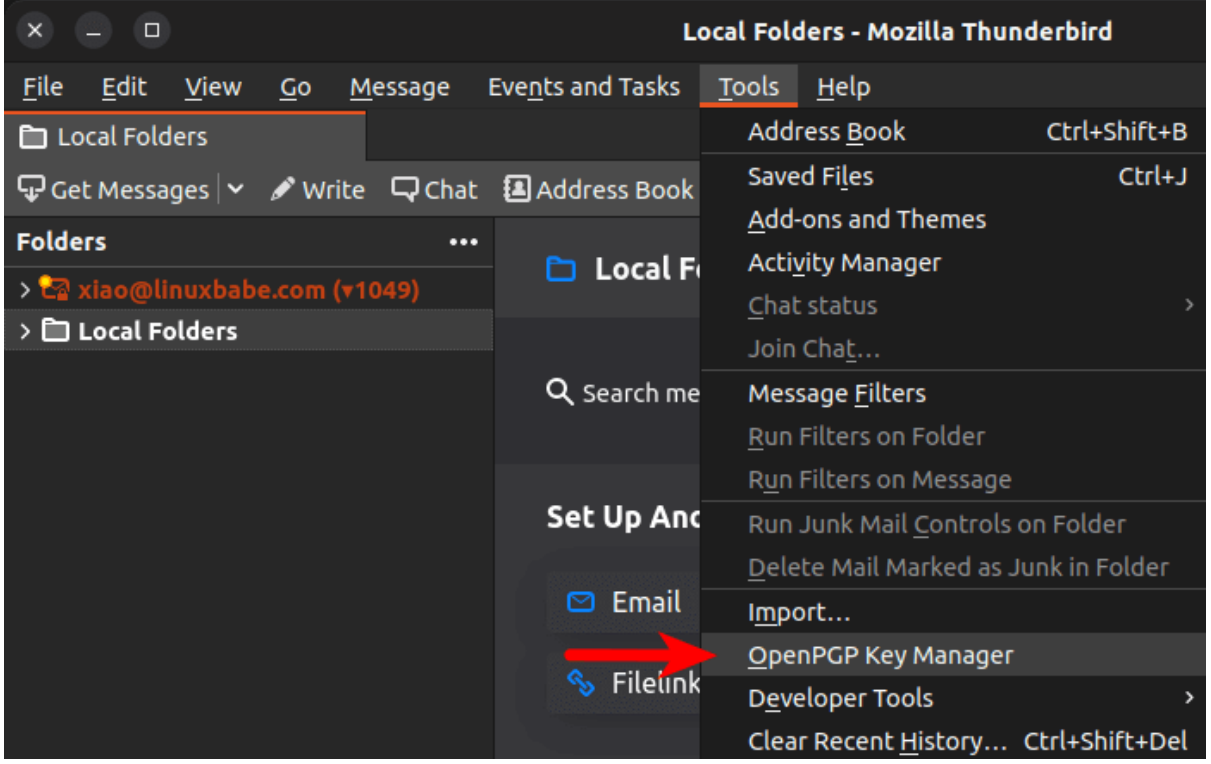
If you follow my previous GPG tutorial, then you should have a key pair managed by GnuPG. Now you need to import it to Thunderbird.

By default, GnuPG stores your private key in encrypted format under the `~/.gnupg/private-keys-v1.d/` directory. You need to unlock your private key, so Thunderbird will be able to import it. Run the following command to unlock your private key, which will be saved in your home directory as `privkey.asc`. You will be asked to enter the key passphrase.

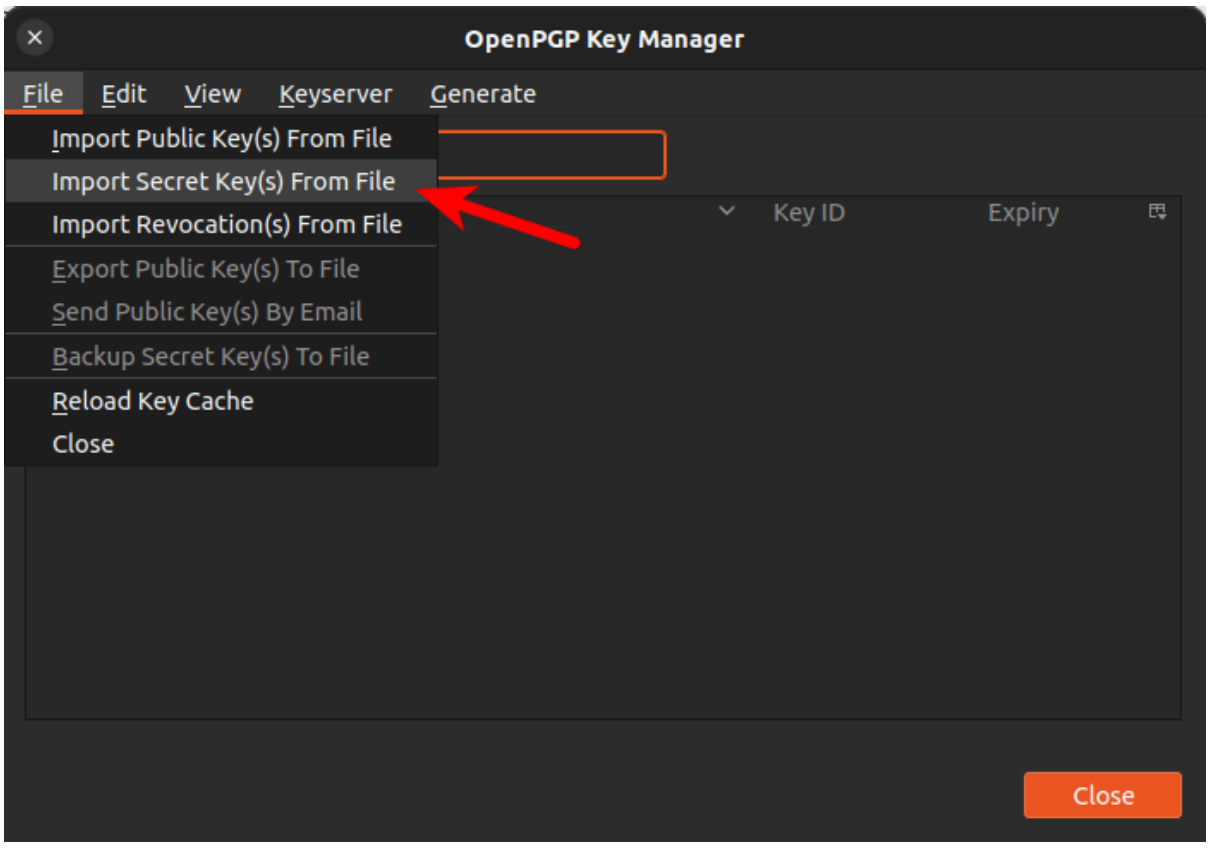
gpg --export-secret-keys --armor user-id > ~/privkey.asc

- user-id is your GPG email address.

Then in the Thunderbird menu bar, select `Tools` -> `OpenPGP key manager`.

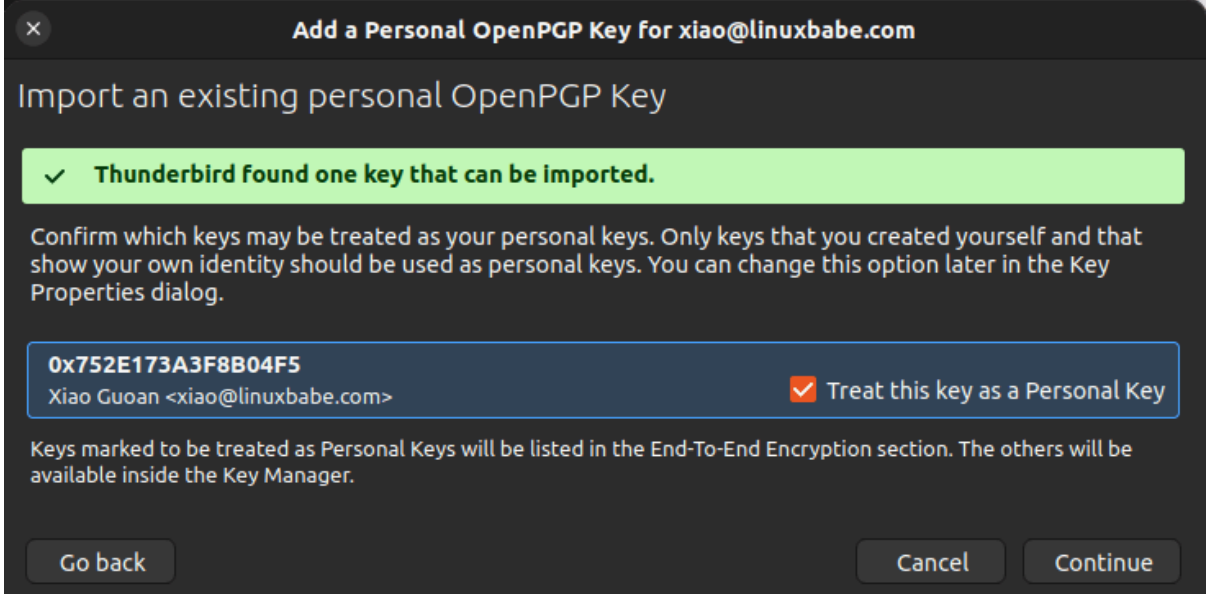


Select `File` -> `Import Secret Key(s) From File`.

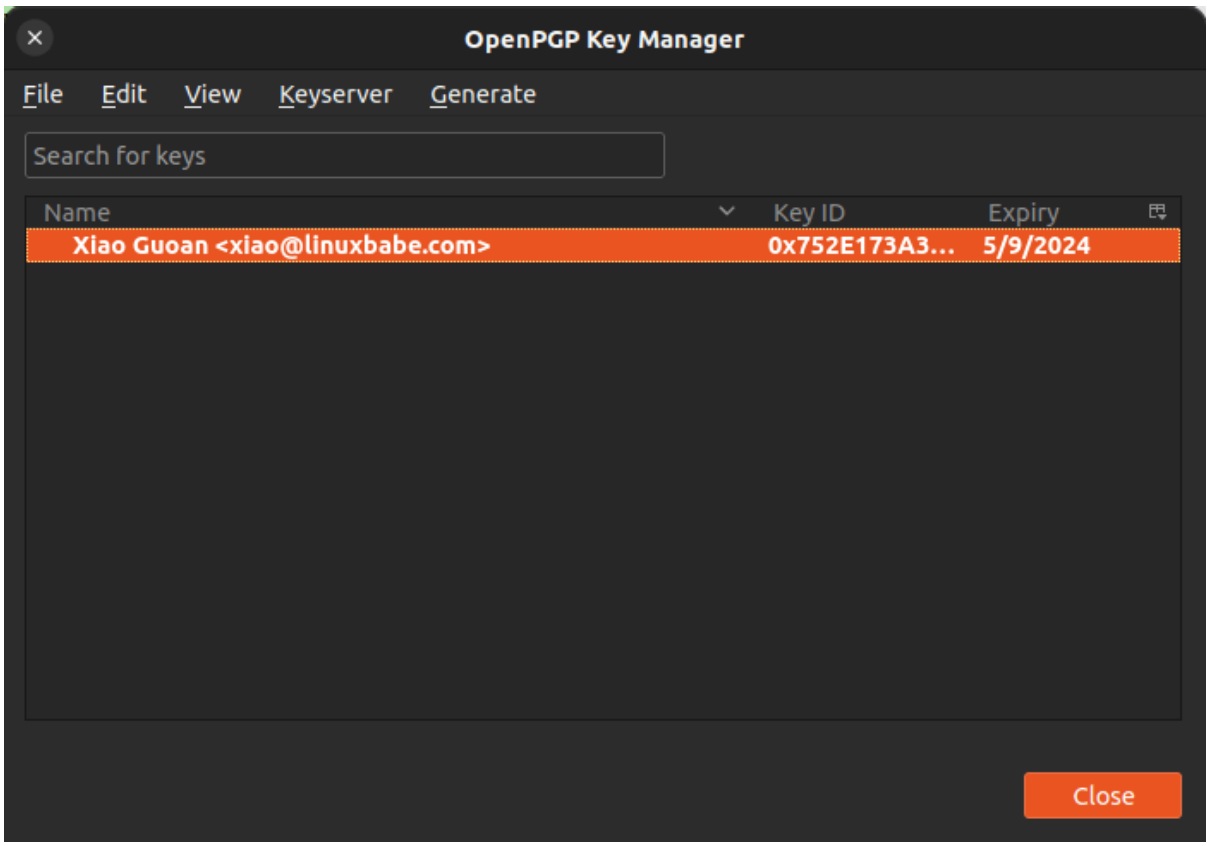


Then select the `privkey.asc` file from your home directory.

Next, click `Continue` button.



You will asked to enter the key passphrase. Once the key is imported, click the `Continue` button, and you will see your personal key in the OpenPGP key manager. Actually this secret key contains both your GPG secret key and public key.



Now you should delete the `privkey.asc` file in your home directory, because private key should not be stored in unencrypted format.

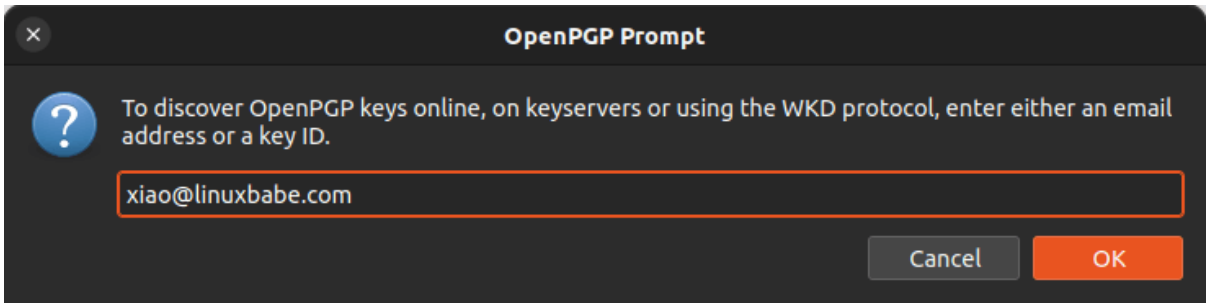
rm ~/privkey.asc

Step 6: Import Recipient's Public Key

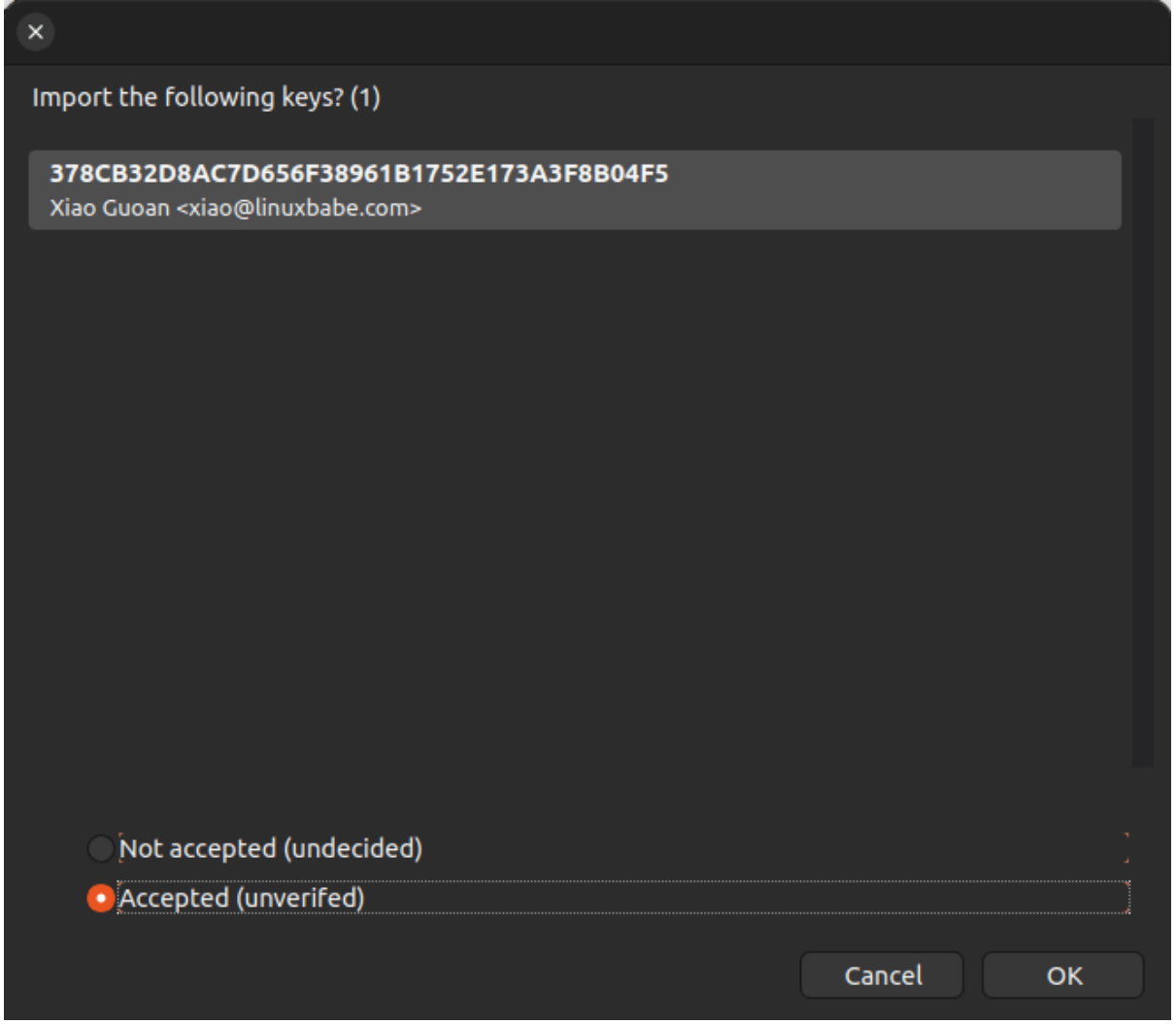
Thunderbird can import public keys in the following ways:

- Import from email attachments
- Import from a file
- Import from a URL
- Search and download the key from a key server (`hkps://keys.openpgp.org`).

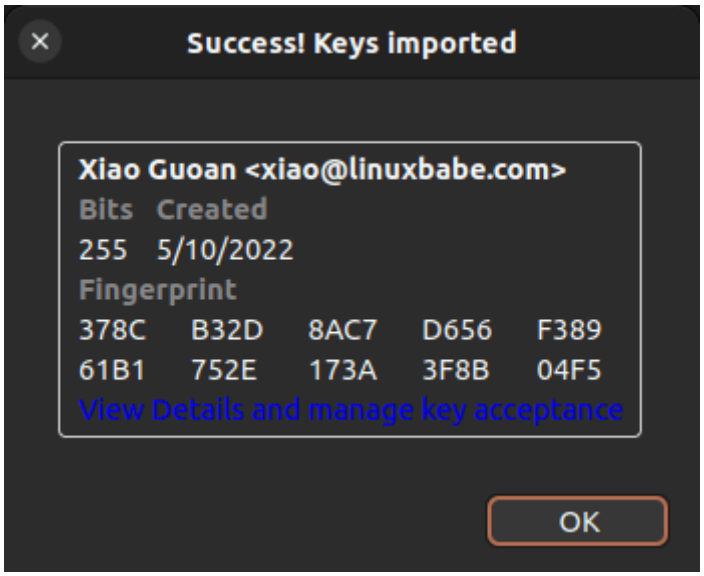
  Ask the recipient how you can import his/her key. For example, I uploaded my public key to the OpenPGP key server, if you want to send me encrypted emails (`xiao@linuxbabe.com`), you can search it in Thunderbird (**Key server** -> **Discover Keys Online**).



  As you can see, it found my public key. Select **Accepted (unverified)** and click **OK** button.



Once it's imported, Thunderbird will show you the fingerprint of this public key. Click the OK button.

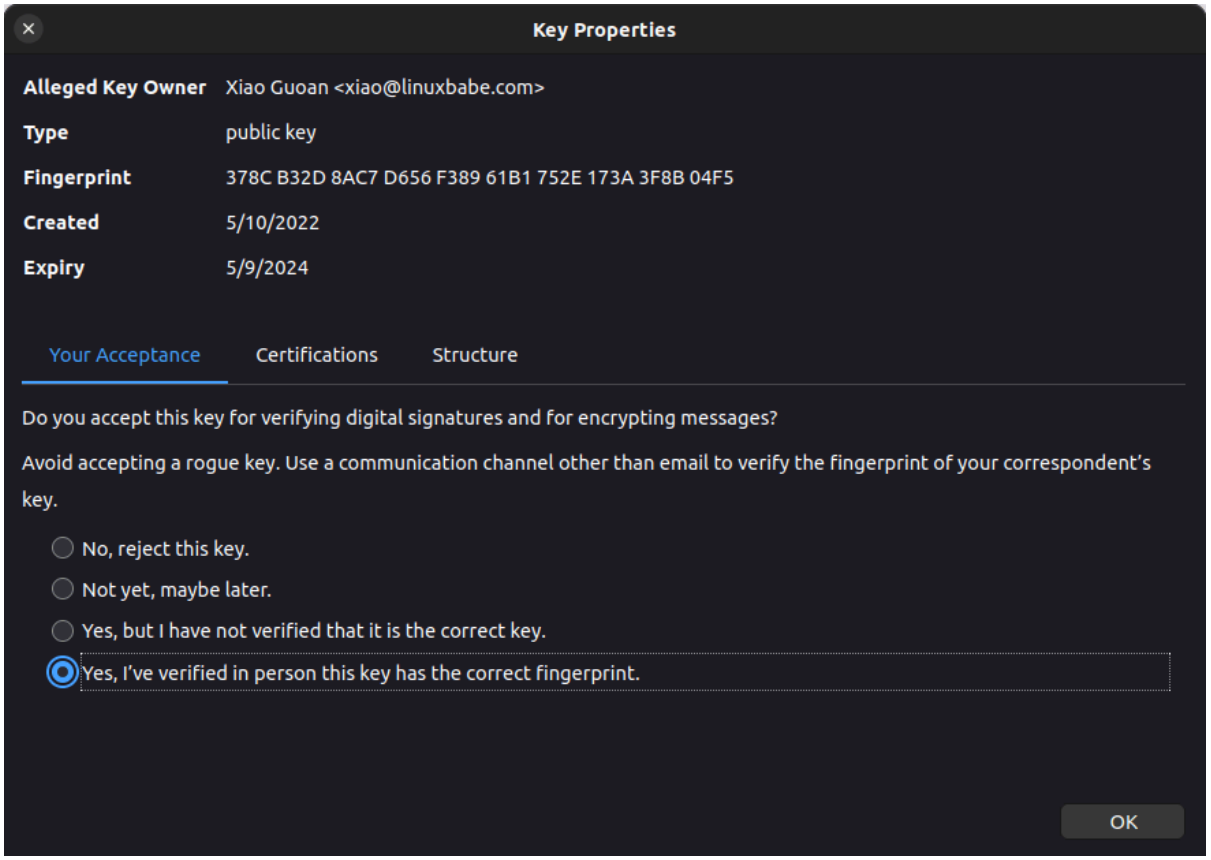


Step 7: Validate Public Keys

When somebody gives you his/her public key, how do you know the public key really belongs to that person? Once you imported another's public key, you should validate the key's authenticity.

In the Thunderbird OpenPGP key manager window, right-click on the recipient's public key and select **Key Properties**. You will see the fingerprint of this public key. You need to contact the key's owner over the phone, in person, or by other means as long as you make sure you contact the key's true owner and you ask the owner what's the fingerprint of his/her key.

Compare the two fingerprints. If the two fingerprints match, then you can be sure it's the correct public key, and you should select **Yes, I've verified in person this key has the correct fingerprint** and click the **OK** button.



By the way, the fingerprint of my public key is `378C B32D 8AC7 D656 F389 61B1 752E 173A 3F8B 04F5`.

Step 8: Share Your Own Public Key

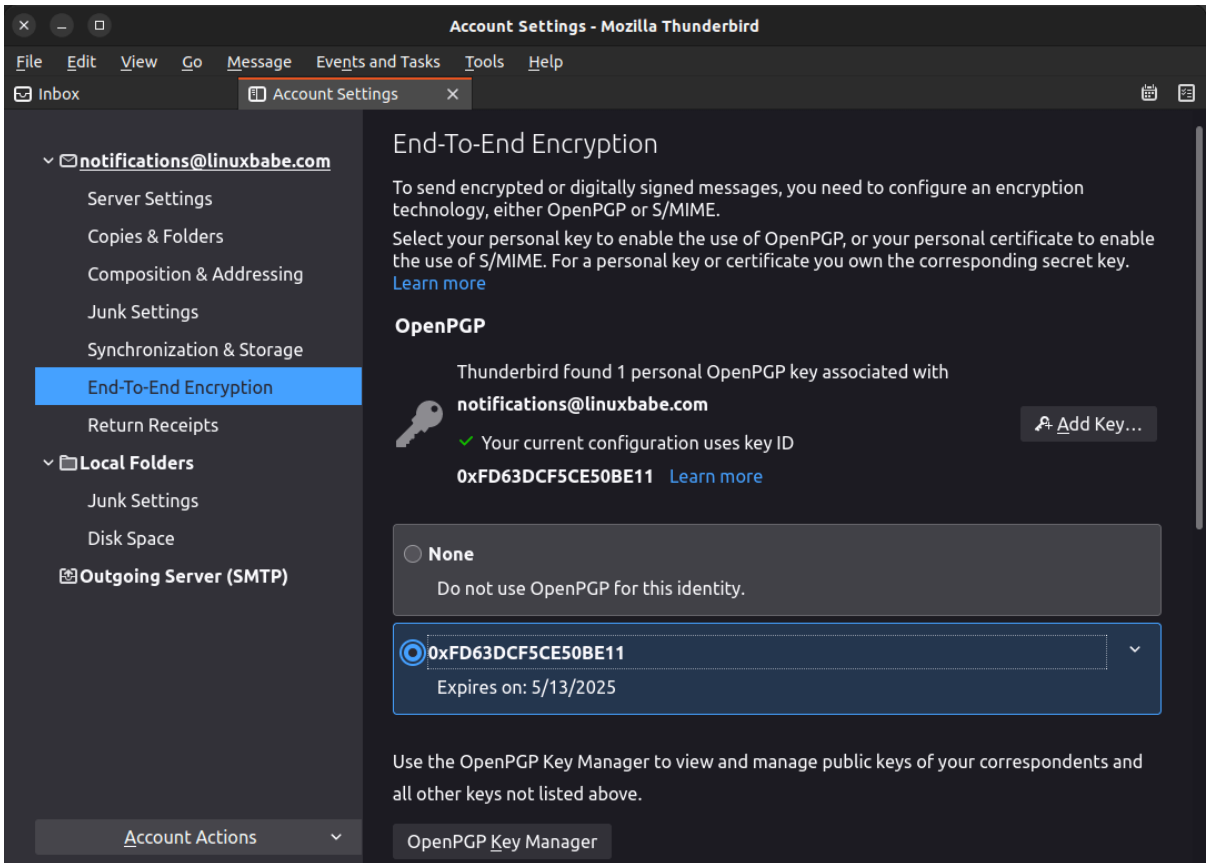
Now you can send the recipient an encrypted email, but the recipient also needs your public key in order to send an encrypted email back to you, so you need to share you public key.

In the Thunderbird OpenPGP key manager, right-click on your own key and select **Send Public Key(s) by Email**. You will be able to

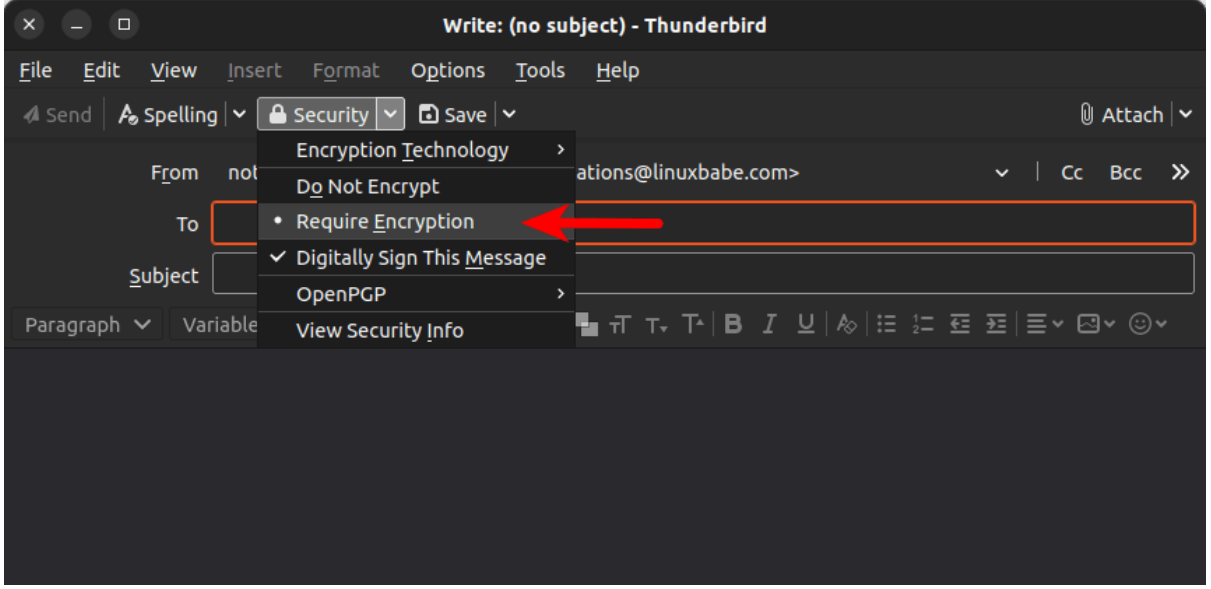
send your public key as an attachment, so the recipient can import it.

Step 9: Send Test Emails

By default, Thunderbird disables OpenPGP encryption. To enable it, go to **Account Settings** -> **End-To-End Encryption**, and select your key for your email account. You can also scroll down, then enable **Require encryption by default** and **Add my digital signature by default**.



Now you can send a test encrypted email. In the email compositing window, select **Security** -> **Require Encryption**.

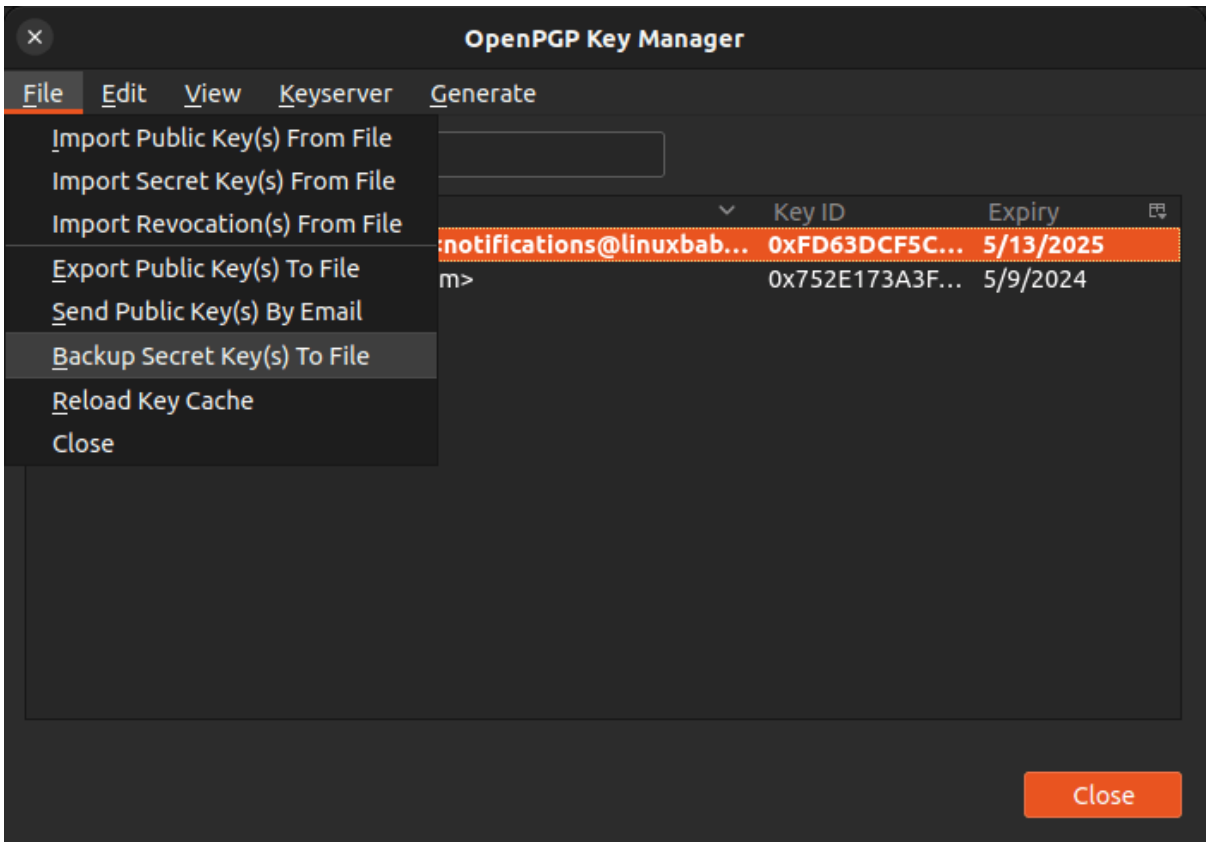


By default, Thunderbird will also sign the email, so not only the email will be encrypted, but the recipient will also know this email really comes from you and hasn't been tampered with.

Thunderbird will also attach your public key to this email.

Step 10: Back Up Your Private Key

If you lose your private key, you won't be able to decrypt your emails. In the OpenPGP key manager window, select your own key and select the File menu -> Backup Secret key(s) to File.



Wrapping Up

Congrats! You can send and receive encrypted emails in Thunderbird. In the next tutorial, you will learn how GPG signatures works.

- A Practical Guide to GPG Part 5: Digital Signature