linuxbabe.com

A Practical Guide to GPG Part 2: Public Key Management

Xiao Guoan (Admin)

9-12 minutes

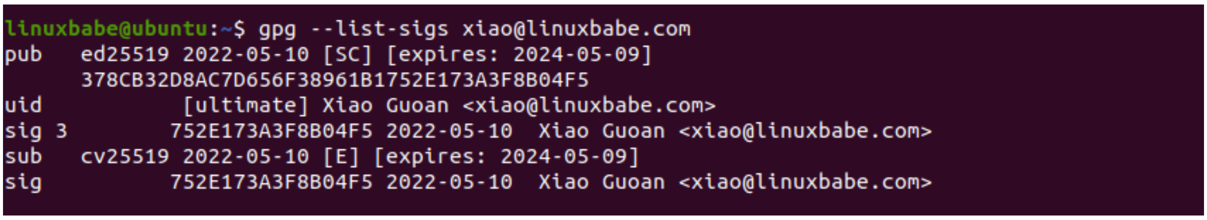
In part 1 of this GPG tutorial series, you learned the benefits of GPG and generated your public/private key pair. In part 2, you will learn how to upload your public key to a key server so others can send you encrypted messages that only can be decrypted with your private key. We will also look at how to import and verify other's public keys and manage your keyring.

Step 1: Check Your Own Public Key

Run the following command to list your own GPG public key. Replace `user-id` with your GPG email address.

gpg --list-sigs user-id

Sample output:



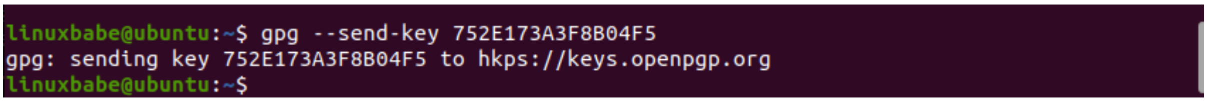
```
linuxbabe@ubuntu:~$ gpg --list-sigs xiao@linuxbabe.com
pub   ed25519 2022-05-10 [SC] [expires: 2024-05-09]
      378CB32D8AC7D656F38961B1752E173A3F8B04F5
uid           [ultimate] Xiao Guoan <xiao@linuxbabe.com>
sig 3        752E173A3F8B04F5 2022-05-10  Xiao Guoan <xiao@linuxbabe.com>
sub   cv25519 2022-05-10 [E] [expires: 2024-05-09]
sig          752E173A3F8B04F5 2022-05-10  Xiao Guoan <xiao@linuxbabe.com>
```

As you can see, my key ID is *752E173A3F8B04F5,* and my key fingerprint is *378CB32D8AC7D656F38961B1752E173A3F8B04F5.*

Step 2: Share Your Public Key on Public Keyserver

Remember you should never share your private key, only share your public key. There're hundreds of public keyservers around the world. Ubuntu has their own. MIT has one. Use the following command to send your public key to a keyserver.

gpg --send-key key-id

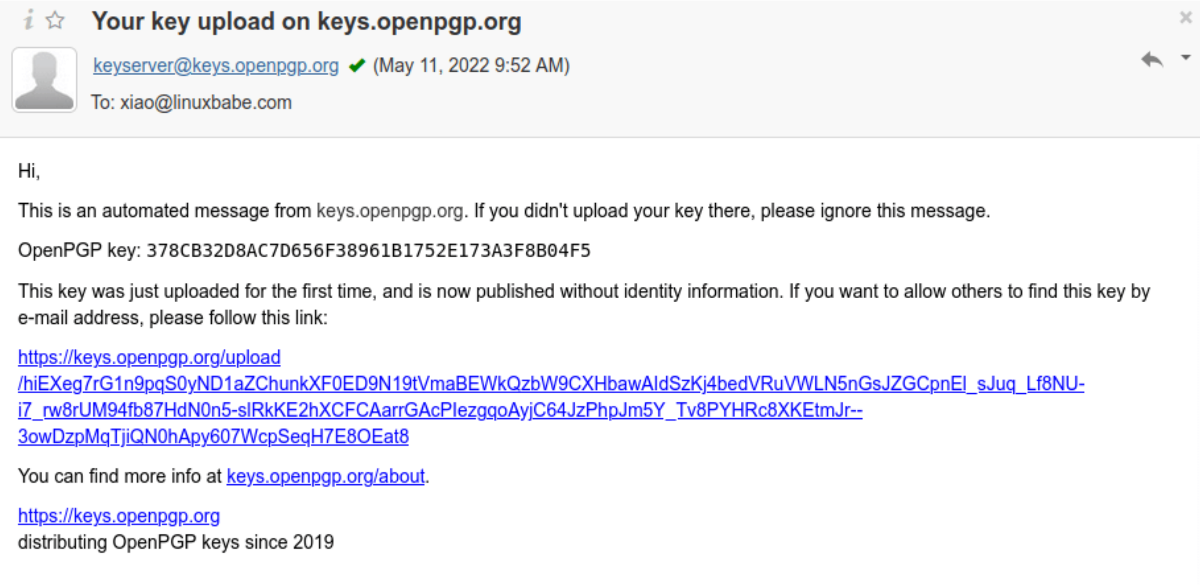


```
linuxbabe@ubuntu:~$ gpg --send-key 752E173A3F8B04F5
gpg: sending key 752E173A3F8B04F5 to hkps://keys.openpgp.org
linuxbabe@ubuntu:~$
```

On Ubuntu, GPG will send your public key to the default keyserver `hkps://keys.openpgp.org`. You have the choice to select a different public keyserver with `--keyserver` option, but I prefer to use the default openPGP keyserver.

gpg --keyserver hkps://keyserver.ubuntu.com --send-key key-id

If your public key is sent to the openPGP keyserver, it will send a notification to your email address.



Your key upload on keys.openpgp.org

keyserver@keys.openpgp.org ✓ (May 11, 2022 9:52 AM)

To: xiao@linuxbabe.com

Hi,

This is an automated message from keys.openpgp.org. If you didn't upload your key there, please ignore this message.

OpenPGP key: 378CB32D8AC7D656F38961B1752E173A3F8B04F5

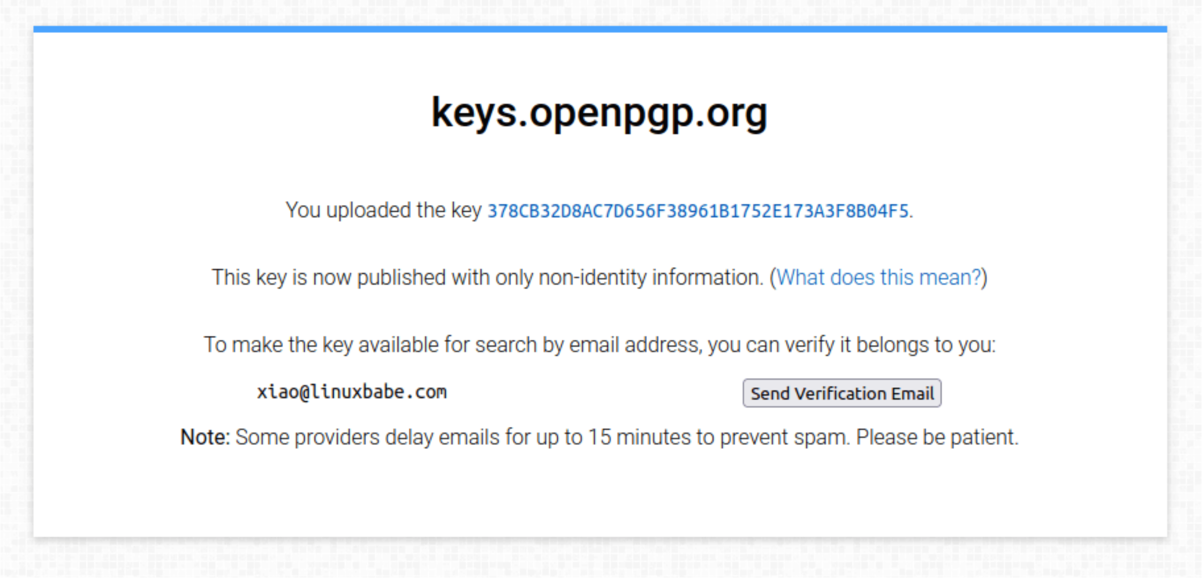
This key was just uploaded for the first time, and is now published without identity information. If you want to allow others to find this key by e-mail address, please follow this link:

https://keys.openpgp.org/upload/hiEXeg7rG1n9pqS0yND1aZChunkXF0ED9N19tVmaBEWkQzbW9CXHbawAldSzKj4bedVRuVWLN5nGsJZGCpnEl_sJuq_Lf8NU-i7_rw8rUM94fb87HdN0n5-slRkKE2hXCFCAarrGAcPlezgqoAyjC64JzPhpJm5Y_Tv8PYHRc8XKEtmJr--3owDzpMqTjiQN0hApy607WcpSeqH7E8OEat8

You can find more info at keys.openpgp.org/about.

https://keys.openpgp.org
distributing OpenPGP keys since 2019

By default, your pubic key is not available for search by email address. If you want others to search your public key by email address, then click the link in the email. Then you will need to verify your email address. This way, an imposter can’t upload a fake key with your email address as the identifier.



keys.openpgp.org

You uploaded the key 378CB32D8AC7D656F38961B1752E173A3F8B04F5.

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

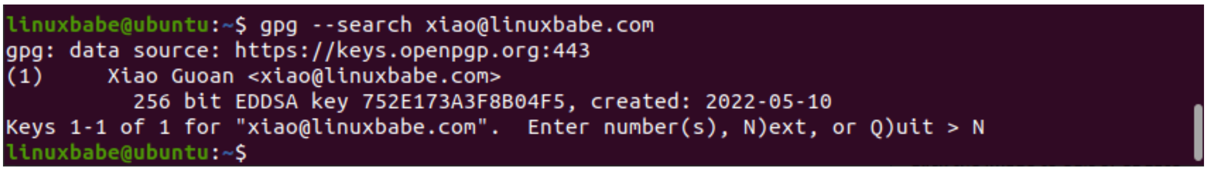
To make the key available for search by email address, you can verify it belongs to you:

xiao@linuxbabe.com

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

After your email address is verified, you can search for your key on the key server.

gpg --search user-id



```
linuxbabe@ubuntu:~$ gpg --search xiao@linuxbabe.com
gpg: data source: https://keys.openpgp.org:443
(1)     Xiao Guoan <xiao@linuxbabe.com>
          256 bit EDDSA key 752E173A3F8B04F5, created: 2022-05-10
Keys 1-1 of 1 for "xiao@linuxbabe.com".  Enter number(s), N)ext, or Q)uit > N
linuxbabe@ubuntu:~$
```

As you can see, it found my public key. When it asks what you want to do with this key, press N and it will quit, because this key is already on your system. If you don't verify your email address, then you can't search the key by email address.

Step 3: Import Others' Public Key to Your Keyring

If you need to send an encrypted message to a recipient with GPG, then you should import the recipient's public key to your keyring. The keyring contains your public key and imported public keys. The keyring file is located at `~/.gnupg/pubring.kbx`.

Import from a file:

You can ask the recipient to give you the public key file and import it with the following command:

gpg --import public-key-file

Import from keyserver

If the recipient’s public key is uploaded to a key server, you can import it from a key server. Use the following command to search public keys on the keyserver. User ID is the recipient’s email address.

```
gpg --search user-id
```

If you know the key ID beforehand, use `--recv-keys` options to import the key from the keyserver.

```
gpg --recv-keys key-id
```

To specify a particular key server, us the `--keyserver` option like below.

```
gpg --keyserver hkps://keyserver.ubuntu.com --search user-id
```

Once you find the requested public key, you can import it to your keyring.

Step 4: Validate Public Keys

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

Here’s how the validation process works:

1. You view the fingerprint of the public key with command: `gpg --fingerprint user-id`
2. You 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.
3. Compare the two fingerprints. If the two fingerprints match, then you can be sure it’s the correct public key.
4. Then you sign the key to certify it as a valid key. To sign a key, use command `gpg --sign-key key-id`

The fingerprint is a hash of public key. Its length is much shorter than the length of public key, therefore it’s easy for you to compare fingerprints. You must have you own private key in order to sign another's public key.

After you sign the other person's public key, you can optionally upload the public key to a key server. This tells the key server that you trust this person's public key, so other people will have more confidence to trust this public key.

```
gpg --send-key key-id
```

However, this also creates a privacy problem, because the world knows that you know the owner of this public key. If you are very careful about privacy, then don't upload this public key, which has your signature on it.

Step 5: Manage Your Keyring

List all keys in your public keyring

```
gpg --list-keys
```

Sample output:

```
pub   ed25519 2022-05-10 [SC] [expires: 2024-05-09]
      378CB32D8AC7D656F38961B1752E173A3F8B04F5
uid           [ultimate] Xiao Guoan <xiao@linuxbabe.com>
sub   cv25519 2022-05-10 [E] [expires: 2024-05-09]
```

List all keys with signature

```
gpg --list-sigs
```

sample output:

```
pub   ed25519 2022-05-10 [SC] [expires: 2024-05-09]
      378CB32D8AC7D656F38961B1752E173A3F8B04F5
uid           [ultimate] Xiao Guoan <xiao@linuxbabe.com>
sig 3        752E173A3F8B04F5 2022-05-10  Xiao Guoan
<xiao@linuxbabe.com>
sub   cv25519 2022-05-10 [E] [expires: 2024-05-09]
sig          752E173A3F8B04F5 2022-05-10  Xiao Guoan
<xiao@linuxbabe.com>
```

To delete a key

```
gpg --delete-key key-id
```

Hint: Most of the time, you can use the fingerprint as key ID.

List Keys in Your Private Keyring

```
gpg --list-secret-key
```

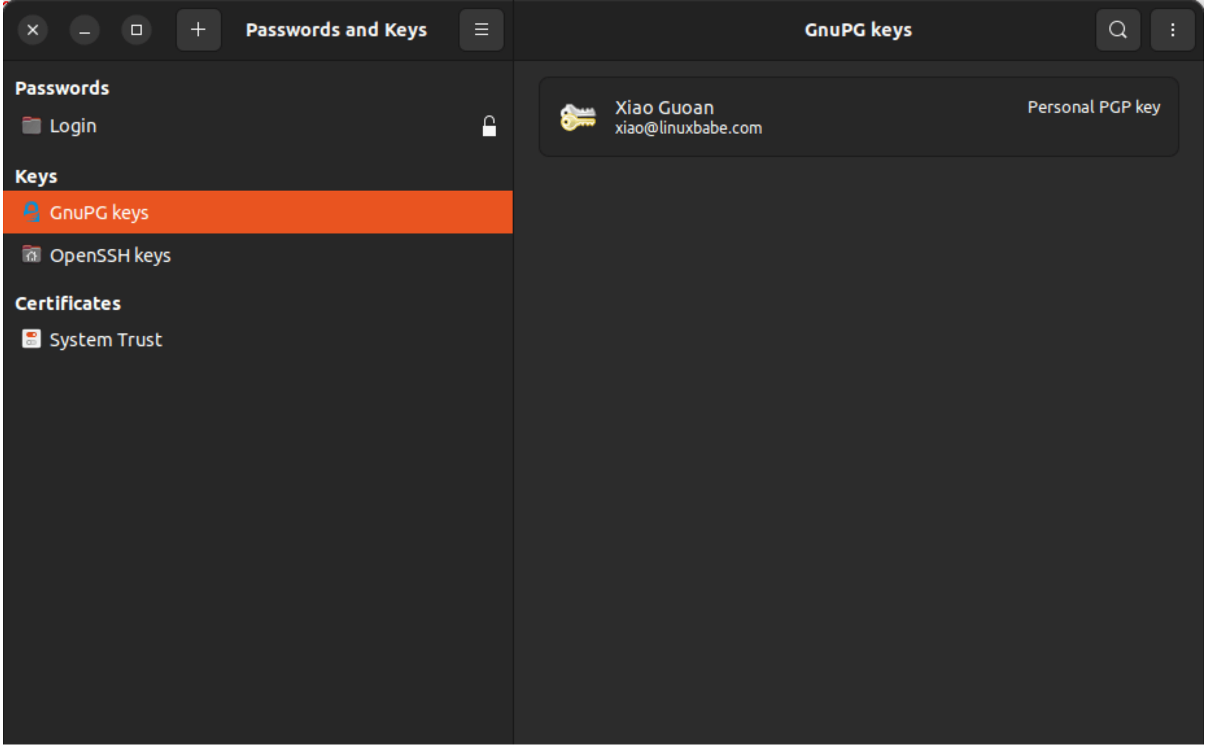
Sample output

```
/home/linuxbabe/.gnupg/pubring.kbx
---------------------------------
sec   ed25519 2022-05-10 [SC] [expires: 2024-05-09]
      378CB32D8AC7D656F38961B1752E173A3F8B04F5
uid           [ultimate] Xiao Guoan <xiao@linuxbabe.com>
ssb   cv25519 2022-05-10 [E] [expires: 2024-05-09]
```

Manage GPG Keys in Seahorse

If you use a GNOME-based desktop environement on Linux, then you can manage GPG keys in *Seahorse*, which is a graphical tool for managing and using encryption keys, passwords and certificates. (If you use KDE desktop, there’s a similar program called KGPG.)

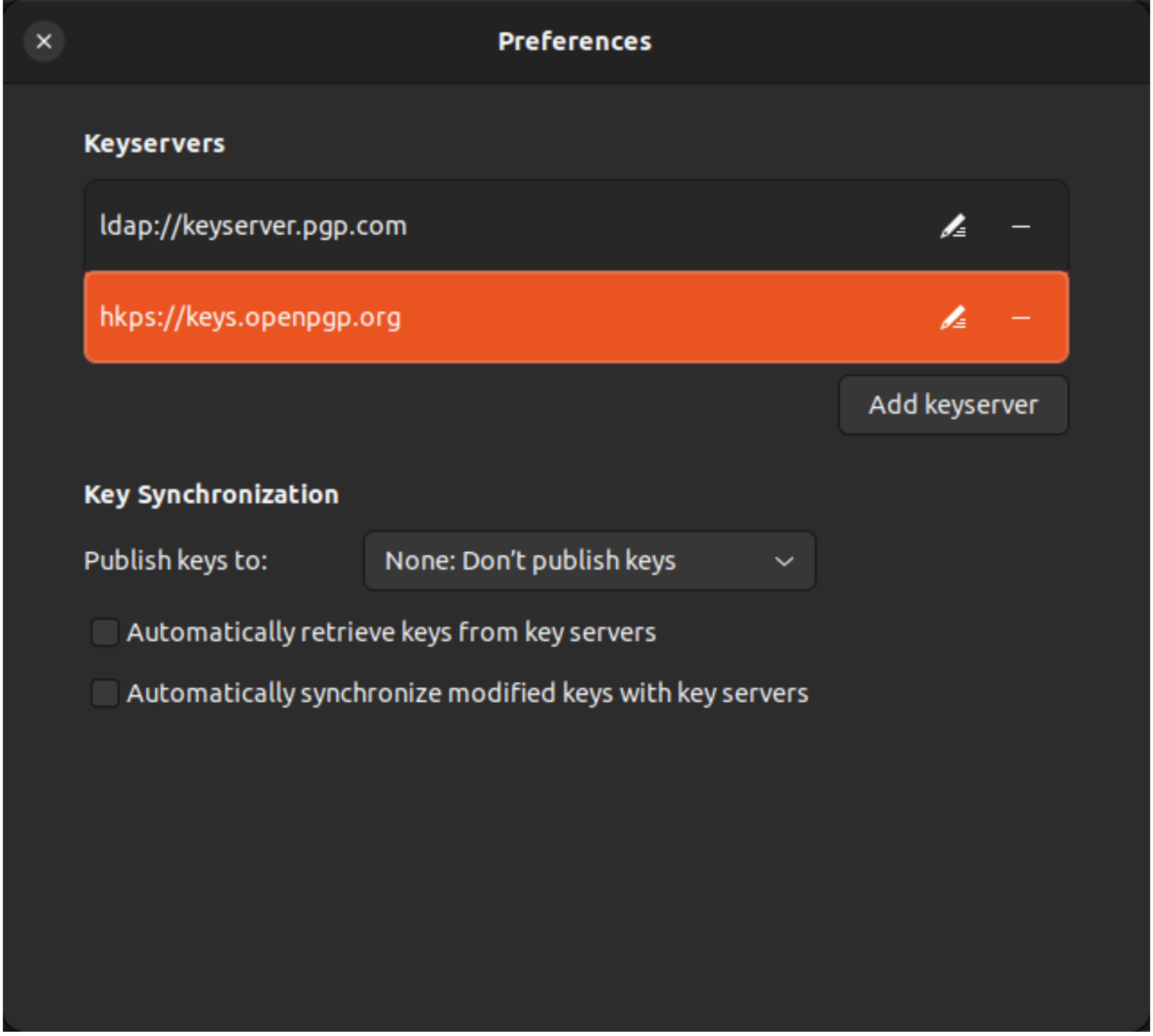
Open Seahorse from your applications menu.



Before starting using it, we need to configure the PGP key server. Click the dropdown menu and go to `Preferences`, you will see there are two default key servers.

- hkp://keyserver.ubuntu.com:11371
- ldap://keyserver.pgp.com

I found the Ubuntu key server doesn’t work, so I change it to the openPGP key server (`hkps://keys.openpgp.org`).



Keyservers

- ldap://keyserver.pgp.com
- hkps://keys.openpgp.org

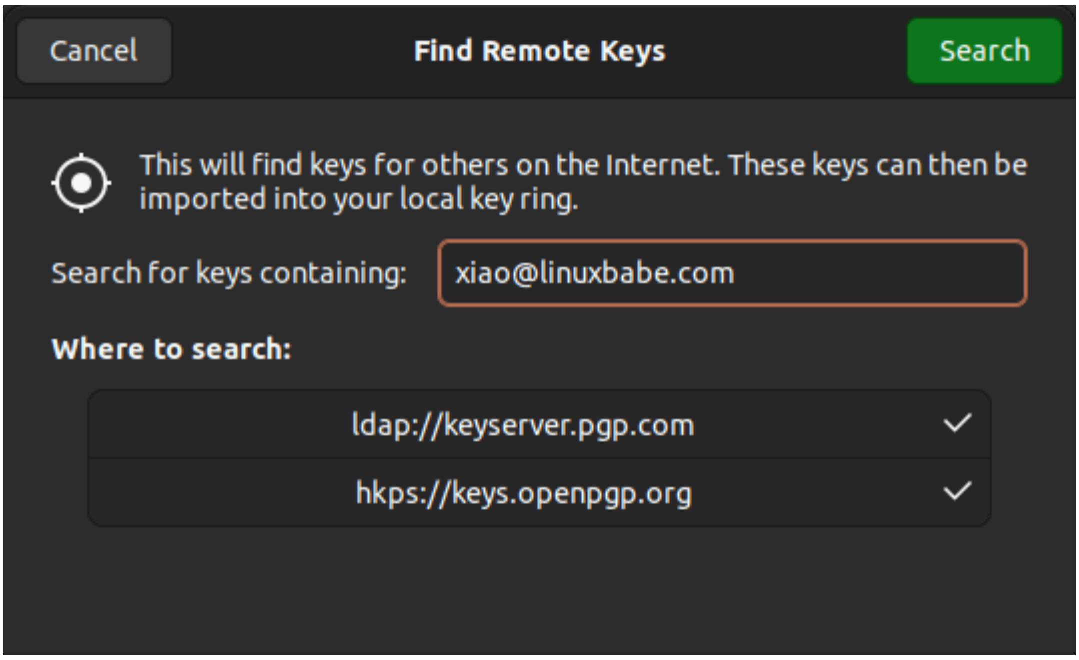
Key Synchronization

Publish keys to: None: Don't publish keys

□ Automatically retrieve keys from key servers

□ Automatically synchronize modified keys with key servers

To import a public key from a key server, click the drop-down menu and select `Find remote keys`. Then enter an email address.



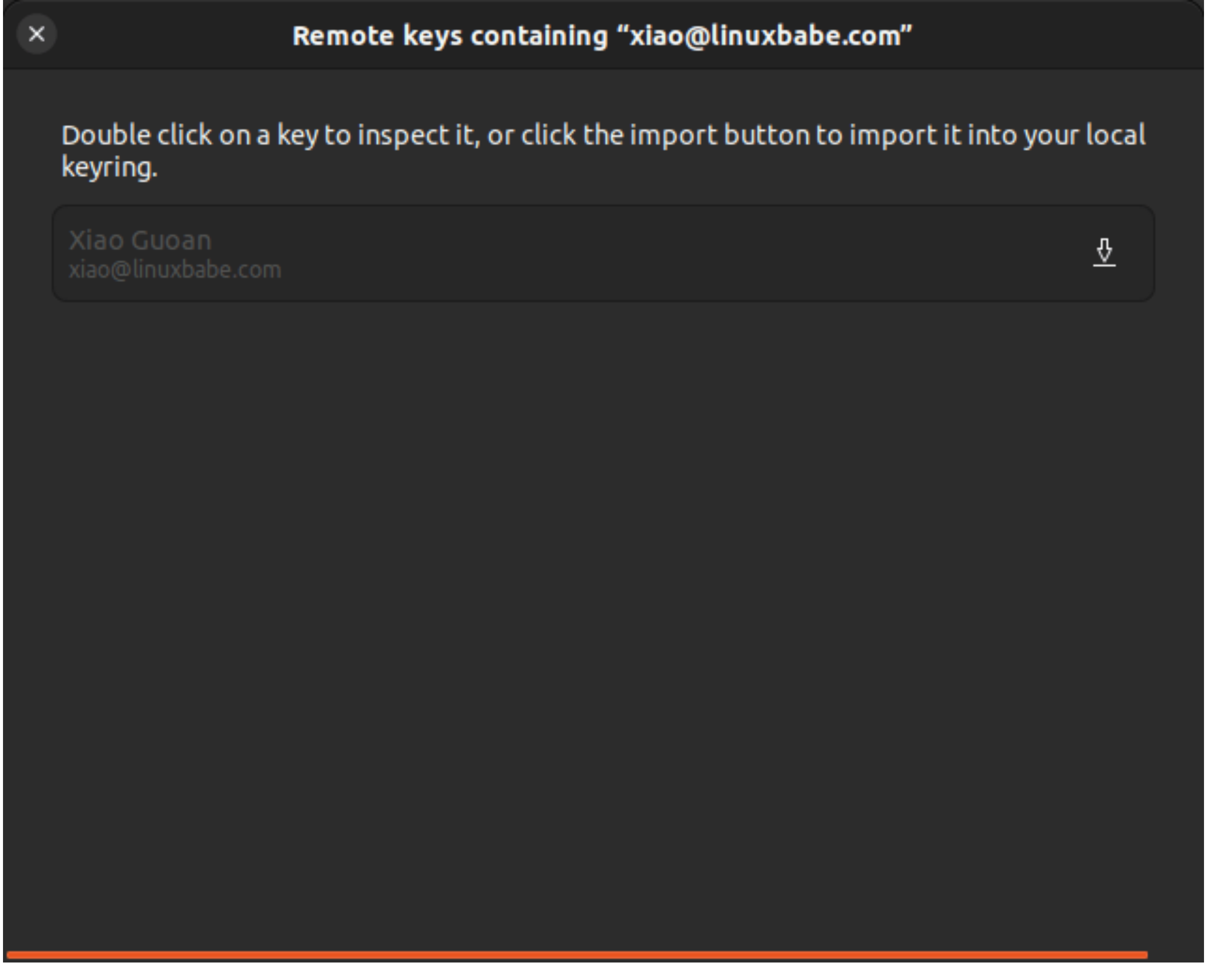
This will find keys for others on the Internet. These keys can then be imported into your local key ring.

Search for keys containing: xiao@linuxbabe.com

Where to search:

- ldap://keyserver.pgp.com ✓
- hkps://keys.openpgp.org ✓

As you can see, it found my public key on the key server. Because this is my own key, so I don't need to import it.



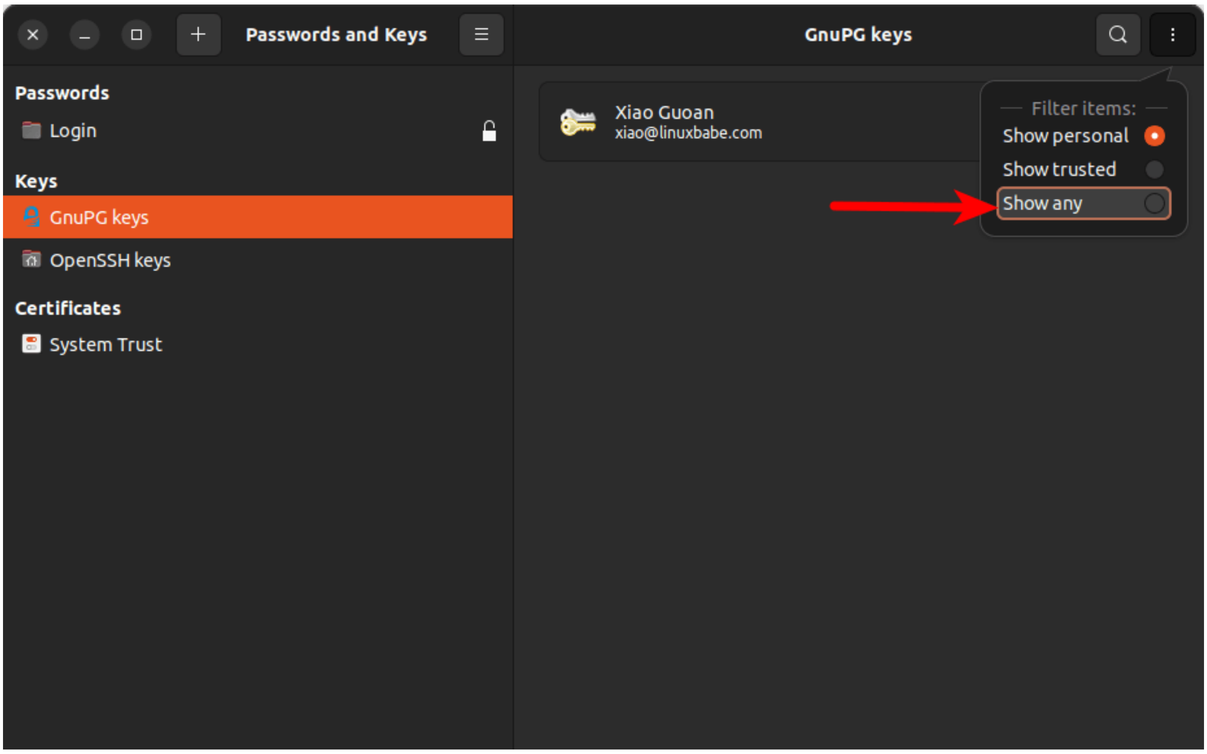
Remote keys containing “xiao@linuxbabe.com”

Double click on a key to inspect it, or click the import button to import it into your local keyring.

Xiao Guoan
xiao@linuxbabe.com

If this is another person’s key, you can click the import button, so it will be added to your key ring. And if you run command `gpg --list-keys`, you can see it’s been added to your key ring.

By default, Seahorse only show your own key. To show other keys, click the `show any` option.



Xiao Guoan
xiao@linuxbabe.com

Filter items:
Show personal ●
Show trusted ○
Show any ○

Right-click on another person’s key and select `Property`, you will be able to check the key’s fingerprint. As explained earlier, you need to contact the key’s owner and verify if it’s the fingerprint is correct.

If the fingerprint is correct, you should sign the public key by clicking the `sign key` button.

How to Extend Key Expiration Date

It’s always a good idea to create a key with an expiration date. Why? If you lose your private key, you can’t decrypt messages anymore, so it’s good to let people know that they should not use the public key after the expiration date.

To extend the expiration date of your key, run the following command, where `user-id` is your GPG email address.

```
gpg --pinentry-mode=loopback --edit-key user-id
```

Select the **primary key**:

```
gpg> key 0
```

Change expiry date:

```
gpg> expire
```

Example:

```
Changing expiration time for the primary key.
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 2y
Key expires at Sat 18 May 2024 10:01:47 AM +08
Is this correct? (y/N) y
```

Then you need to enter the passphrase of your secret key to verify you are the owner.

Next, select the **subkey**.

```
gpg> key 1
```

Change expiry date:

```
gpg> expire
```

Example:

```
Changing expiration time for the subkey.
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 2y
Key expires at Sat 18 May 2024 10:01:47 AM +08
Is this correct? (y/N) y
```

Save the changes.

```
gpg> save
```

Show your key id.

```
gpg --list-sigs user-id
```

Upload the new key to the key server.

```
gpg --send-key key-id
```

The OpenPGP key server will automatically replace the old key with your new key.

How to Use the Revocation Certificate

If your private key is compromised, you can generate a new key pair and then use the revocation certificate to let everyone know that you don’t use the old key anymore.

On Linux, there’s a default revocation certificate stored under `~/.gnupg/openpgp-revocs.d/` directory. You can generate a new one with the following command:

```
gpg --output revocation.rev --gen-revoke key-id
```

Then import it to your keyring.

```
gpg --import revocation.rev
```

Upload the revoked key to the key server.

```
gpg --send-key key-id
```

The OpenPGP key server will remove your email address from its database. Other people can still search this key by key ID, but when they import it to their keyring, GPG will show a `revoked` status.

Next Step

In this part, you learned how to upload public keys, import other's keys, and key validation. In part 3 of this GPG tutorial series, we will learn how to encrypt and decrypt messages with GPG.

- A Practical GPG Guide Part 3: Encrypt and Decrypt Files