OpenPGP Applet

Tails includes a custom applet, called *OpenPGP Applet*, to manipulate text using OpenPGP.

It is unsafe to write confidential text in a web browser since JavaScript attacks can access it from inside the browser. You should rather write your text in a separate application, encrypt it using *OpenPGP Applet*, and paste the encrypted text in your browser, before sending it by email for example.

When using *OpenPGP Applet* to encrypt emails, non-ASCII characters (for example non-Latin characters or characters with accents) might not display correctly to the recipients of the email.

If you are going to encrypt emails often, we recommend you to set up Thunderbird instead.

OpenPGP Applet is located in the notification area.

With *OpenPGP Applet* you can:

- Encrypt text with a passphrase
- Encrypt and sign text with a public key
- Decrypt and verify text

> If you have GnuPG keys stored in Persistence since before Tails 4.1 (December 2019), you should update your OpenPGP keyserver configuration to use safe keyservers.

Managing your OpenPGP keys

You can manage your OpenPGP keys using the *Passwords and Keys* utility, also called *Seahorse*.

To open the *Passwords and Keys* utility, you can either:

- Click on *OpenPGP Applet* and choose **Manage Keys**.
- Choose **Applications ▸ Utilities ▸ Passwords and Keys**.

To list the public OpenPGP keys in your keyring:

1. Choose **GnuPG keys** in the sidebar of the **Passwords and Keys** utility.

Importing new OpenPGP public keys

Importing OpenPGP public keys using the *Passwords and Keys* utility is broken since Tails 4.0 (October 2019). (#17183)

Do so on the command line instead:

1. Download the OpenPGP public key that you want to import.
2. Choose **Applications ▸ System Tools ▸ Terminal** to open a *Terminal*.
3. Execute the following command to import the OpenPGP public key that you downloaded. Replace:
   - ***openpgp-public-key.asc*** with the path to the OpenPGP public key.

     > If you are unsure about the path to the OpenPGP public key, you can insert the correct path by dragging and dropping the OpenPGP public key

from the *Files* browser onto the *Terminal*.

```
gpg --import openpgp-public-key.asc
```

You should get something like this:

```
gpg --import '/home/amnesia/Tor Browser/0x1DCBDC01B44427C7.asc'
```

The output of this command should look like this:

```
gpg: key 0x1DCBDC01B44427C7: public key "Robert J. Hansen
gpg: Total number processed: 1
gpg:               imported: 1
```

4. The imported OpenPGP public key does not appear in the *Passwords and Keys* utility but should appear in the list of keys available for encryption when encrypting text with a public key using *OpenPGP Applet*.

Mirror: tails.boum.org