Encrypt Emails with OpenPGP in Thunderbird

Article URL
Encrypt Emails with OpenPGP in Thunderbird

Author
SecurityHome.eu

Published: 11 February 2026

Last updated on 12 February 2026.

Â

Encrypt Emails with OpenPGP in Thunderbird

Thunderbird includes built-in OpenPGP support from version 78. It can encrypt your emails and also add digital signatures to your emails.
You can check thunderbird version in : *Help -> About Thunderbird.*

First step Generate or Import GPG Key Pair

you can generate one right in Thunderbird.
In the Thunderbird menu bar, select *Tools -> OpenPGP key manager*

.

Then select *Generate -> New Key Pair*

. (you can generate a different key pair for each email-account)

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 considered more secure, so select ECC (Elliptic Curve) as the key type.

Click *Generate Key*

button. You will be asked to confirm, click *Confirm* button.

Your key pair will be generated and 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 can extend the expiration time in the Key Properties window.

Import your own key

If you have a PGP key pair (from Gnu PGP), you can import it.

If you have a key generated by another program,
Like GnuPGP, you first need to export it.
for GnyPGP, you can use the command:

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

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

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

.

Select the *privkey.asc*

file
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. (this contains both your GPG secret key and public key).

Delete the *privkey.asc*

file in your home directory, because private key should not be stored in unencrypted format.

```
rm ~/privkey.asc
```

Enable encrypted mail

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.

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.

Web Key Directory (WKD)

This step is for website owners.
If you own the domain, you can plublish the public keys for emails of the domain, on your own website.
Ideally a Web Key Directory will be created and maintained through a web service, but small organizations or individuals may want to just host a WKD without a service,
instead relying on a flat file structure which must be recreated whenever a public key changes.

You first have to export your key from Thunderbird.
In the OpenPGP key manager window, select your own key and select the *File/ menu -> Backup Secret key(s) to File*

.

First Import the key in GPG (GNU Privacy Guard)

```
gpg --import file_name.asc
```

You can verify with:

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

The name of the file will be hash of the user-part of the email-address.
(z-base-32 encoded SHA-1 hash of the lowercase local part of the email address.)
can be created with

```
gpg --with-wkd-hash --fingerprint [EMAIL]
```

You get something like this:

```
pub   ed25519 2026-02-07 [SC] [expires: 2029-02-06]
      7D13 AB84 1FFA 3158 4480  0D60 02F9 A408 59BE 7D98
uid           [ unknown] Securityhome.eu
              kd39y8fkyw5j8uubuicshffo9hhodk4j

@securityhome.eu
sub   cv25519 2026-02-07 [E] [expires: 2029-02-06]
```

Export the file:

```
gpg --no-armor --export [EMAIL] > [file-name=hash]
```

example:

```
gpg --no-armor --export webmaster@securityhome.eu > kd39y8fkyw5j8uubuicshffo9hhodk4j
```

You will need a webserver, with https for security.

You can puplish the public keys in
https://openpgpkey.example.com/.well-known/openpgpkey/example.com/hu/

or
https://example.com/.well-known/openpgpkey/hu/

if you dont have access to you DNS to add openpgpkey.example.com/.

Additionally a file named "policy" needs to be created (under .well-known/openpgpkey/policy).
it is required, but can be empty.

You can test it on the site https://wkd.dp42.dev/

Back Up Your Private Key

A good practice, is always have backups.
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*

.
And keep it in a safe place.

Other email clients:
https://www.openpgp.org/software/