

HOW TO SECURE YOUR EMAILS WITH PGP?

Introduction

Internet has been designed for communication, not for security. Security makes communication harder and more restrictive. But since the Internet is the mirror of our society, it's sometimes a good choice to restrict a communication to a small group of trusted people...

PGP basics

For detailed information about how PGP works please refer to: http://en.wikipedia.org/wiki/Pretty_Good_Privacy. To make it digestible, let's summarize it by the following points:

- To send and receive encrypted emails, everyone must have a PGP key,
- A PGP key is made of a Public key and a Private Key,
- The public key is meant to be public, so you can send it to anyone and upload it to an Internet page,
- The private key **_MUST NOT_** be sent to anyone and must be saved in a safe place nobody can access but you.
- To send a encrypted email to somebody, your friend has to send you his/her public key first,
- To receive encrypted emails, you have to send your friend your public key,
- If you send a mail to someone who hasn't got a PGP key, then this mail will be sent in "Clear"

What you need

Vegaplanet

An **email account** with an **IMAP** and **SMTP** access is required for this to work. Vegaplanet can provide you with a free and unlimited email address. The server is located in Switzerland (legally outside the EU). Your mails will be stored encrypted on the Vegaplanet server and not on your local computer.

Worldwide services such as Gmail, Yahoo, Hotmail as well as local services such as Eircom.net shouldn't be considered as regular email accounts and shouldn't be used for very private communications.

Mozilla Thunderbird

Good points

- It's an efficient and open source email client including a efficient spam filter,
- Runs on almost every flavour of Windows, Linux, UNIX and MacOS,
- All versions are compatibles between each other so you only have one folder to backup and restore in case you want to migrate your mails and preferences to another computer,
- Supports a wide variety of plug-ins including PGP/GPG for mail encryption.

Bad points

- When using a software email client such as Thunderbird, you lose some of the flexibility of webmail services such as Gmail, yahoo and hotmail. It means you might not be able to read your encrypted emails from an Internet café or your workplace (unless you install another copy of Thunderbird there, which introduces some issues about your privacy). As a result, you'll only be able to read and send your encrypted emails from your personal computer.

Enigmail & GnuPG

Good points

- This plug-in is very stable and well integrated to Thunderbird,
- Runs on Windows, Linux, UNIX and MacOS,
- Comes with a very efficient Key management,
- Enigmail is open source.

Getting started

Installation on Linux

Linux users should install Thunderbird and Enigmail using their package manager. The installation process differs according the Linux flavour you're using. Here are the following packages to install:

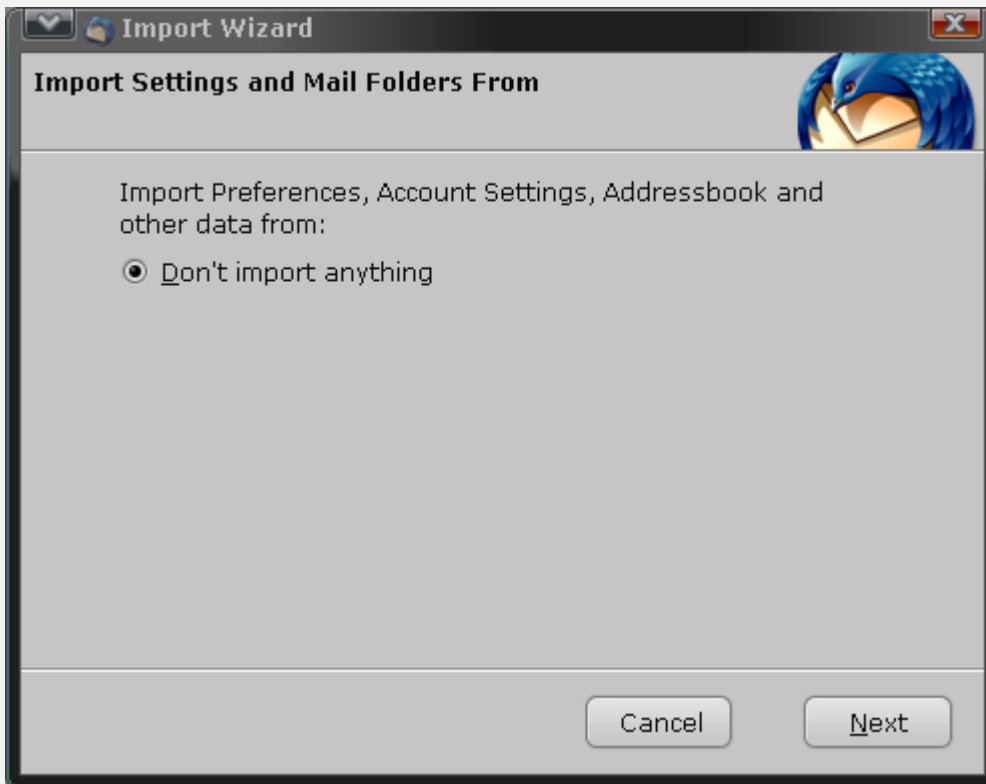
- mail-client/mozilla-thunderbird
- app-crypt/gnupg
- x11-plugins/enigmail

Installation on windows

- **Download** the Enigmail plug-in for Mozilla Thunderbird at the following location: <http://enigmail.mozdev.org/download>
- **Download** GnuPG for windows at the following location: <ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.9.exe>
Install GnuPG for Windows using the defaults settings,
- **Download** Mozilla Thunderbird at the following location: www.mozilla.com/thunderbird
Install Mozilla Thunderbird,
- Once Thunderbird is installed on your computer, **you can delete the installer file.**

Configuration

Start **Thunderbird**, a wizard will show up and will ask you some questions:



Choose the "**Don't import anything**" option, then click "**Next**".

Account Wizard

Identity

Each account has an identity, which is the information that identifies you to others when they receive your messages.

Enter the name you would like to appear in the "From" field of your outgoing messages (for example, "John Smith").

Your Name:

Enter your email address. This is the address others will use to send email to you (for example, "user@example.net").

Email Address:

Cancel Back Next

Enter your nickname (Don't use your real name!) and your email address, then click "**Next**".

Account Wizard

Server Information

Select the type of incoming server you are using.

POP IMAP

Enter the name of your incoming server (for example, "mail.example.net").

Incoming Server:

Enter the name of your outgoing server (SMTP) (for example, "smtp.example.net").

Outgoing Server:

Cancel Back Next

Tick the **"IMAP"** button, enter **"mail.vegaplanet.org"** as the **"Incoming"** and **"Outgoing server"** as above, then click **"Next"**.



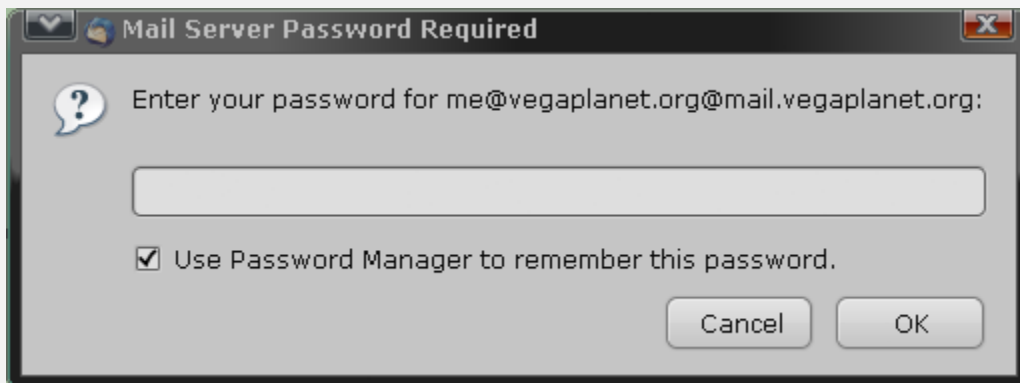
Enter your email address again, then click "**Next**".



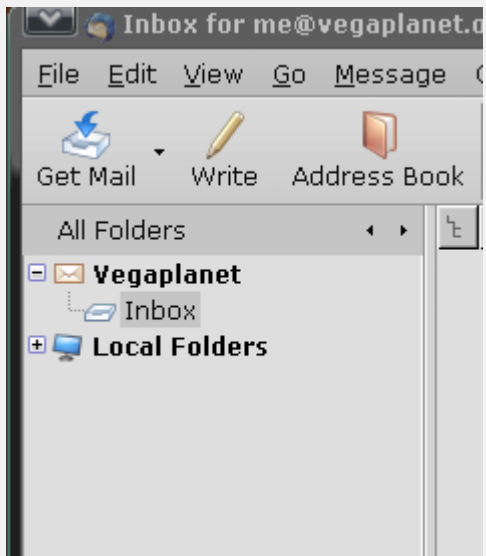
Give "**Vegaplanet**" as the account name, then click "**Next**".



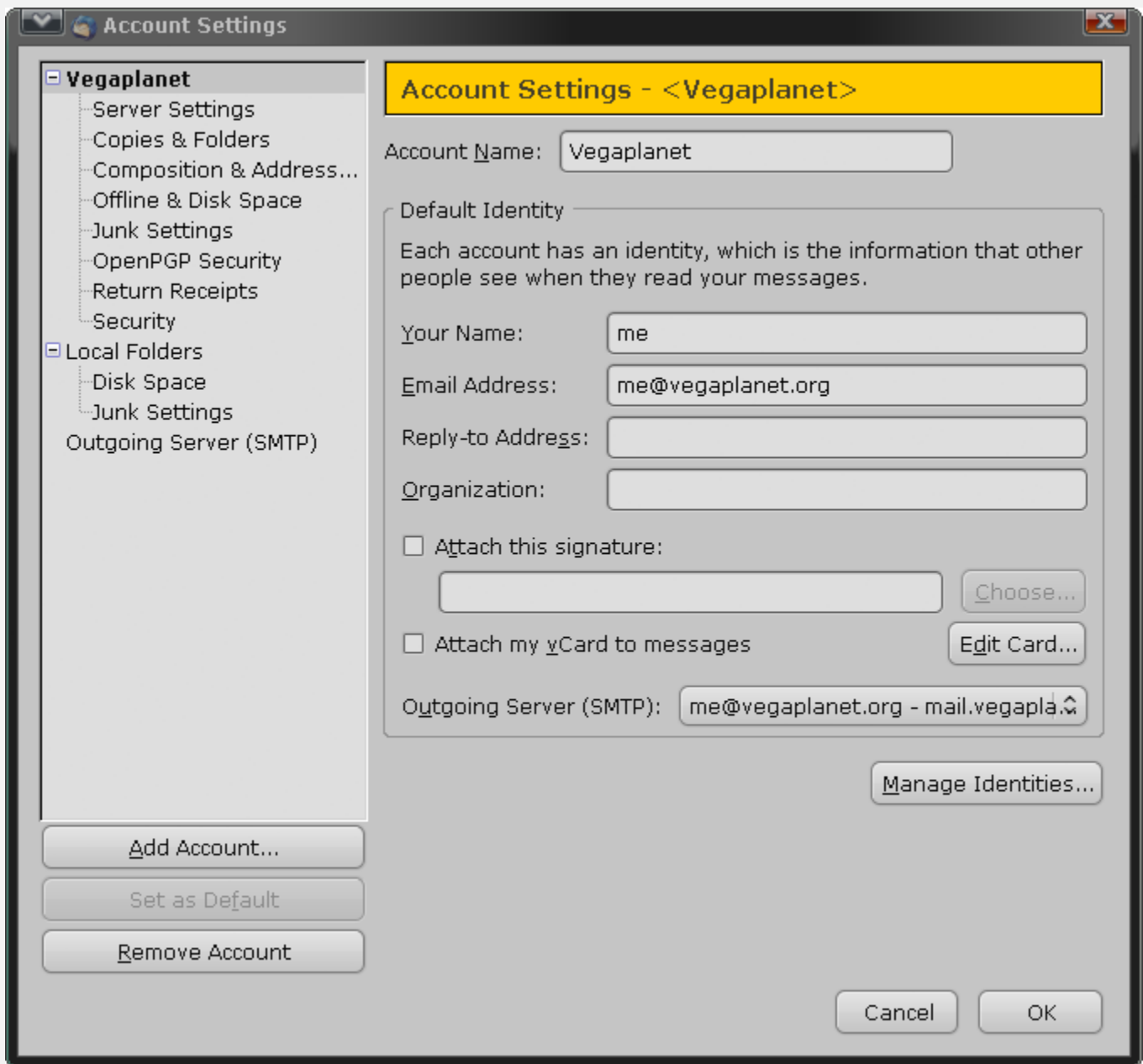
Click "**Finish**"



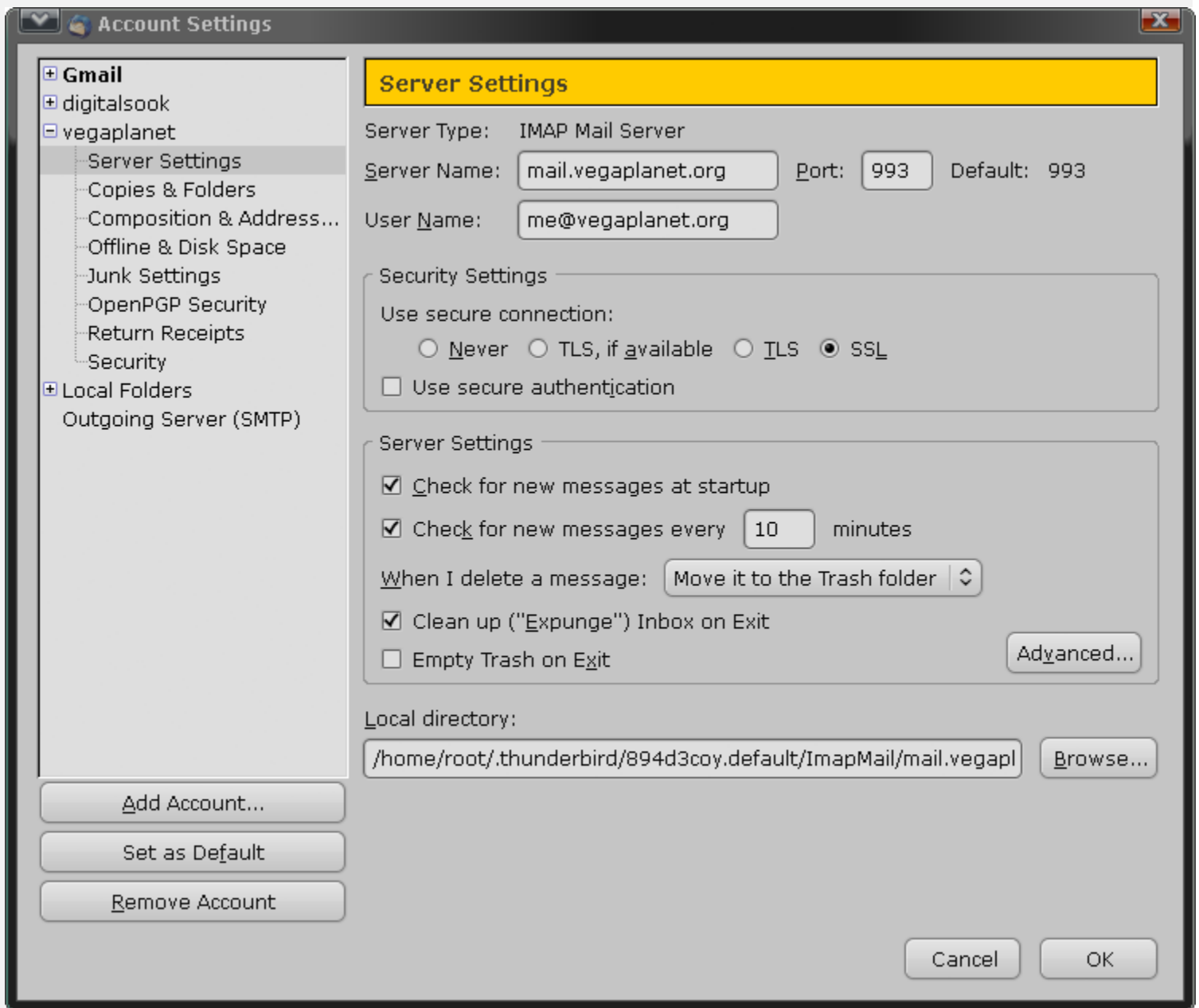
This dialog box will show up. **Give your password**, then click "**OK**".
If everything goes right, Thunderbird will download your mails.
If you don't see any mails, don't panic, your mailbox is empty ;)
The most important thing in this part is that no error message shows up.



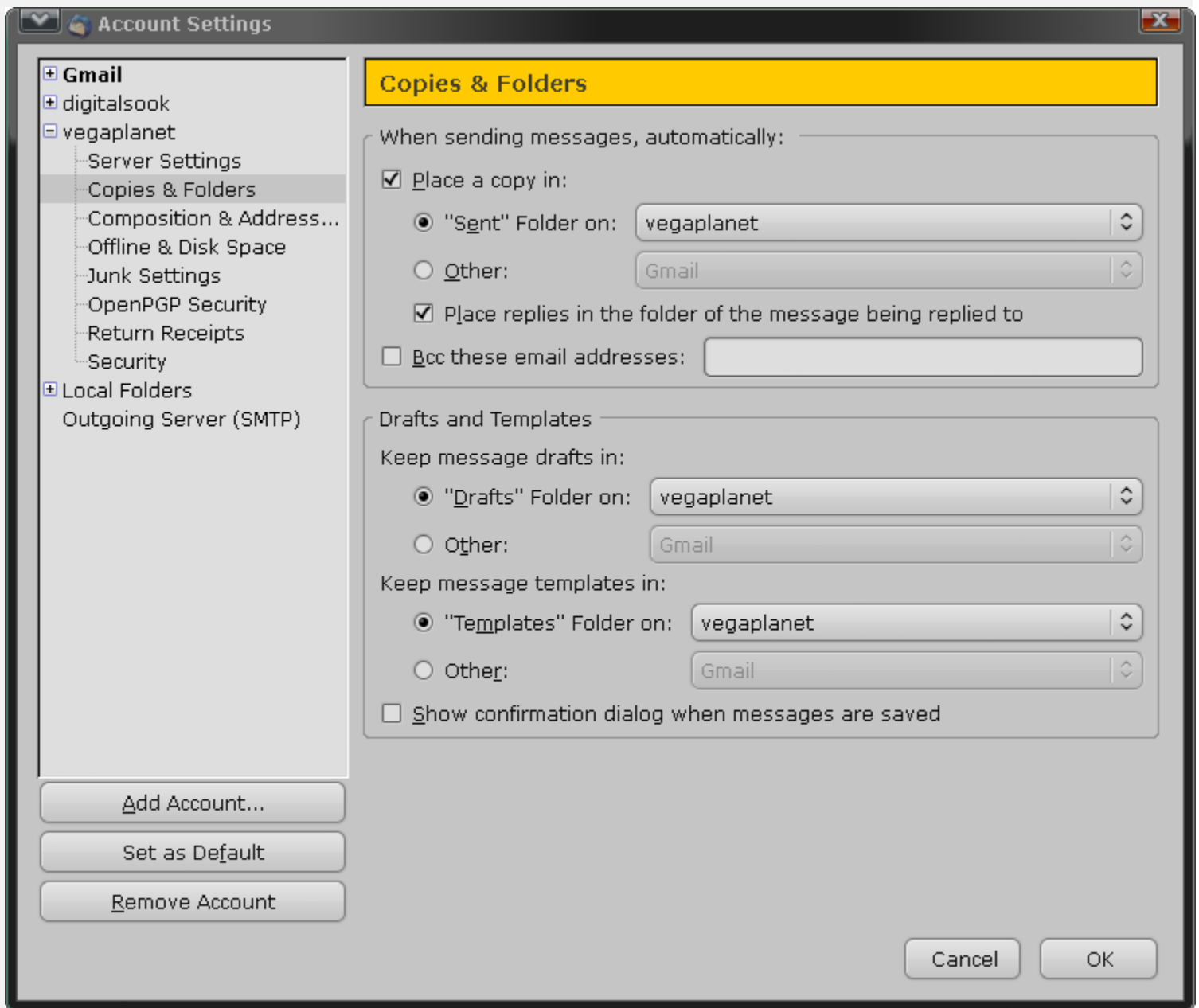
In the left part of the Thunderbird window, **right click on "Vegaplanet"**, select "**Properties**", then make sure the configuration looks like the screenshots below:



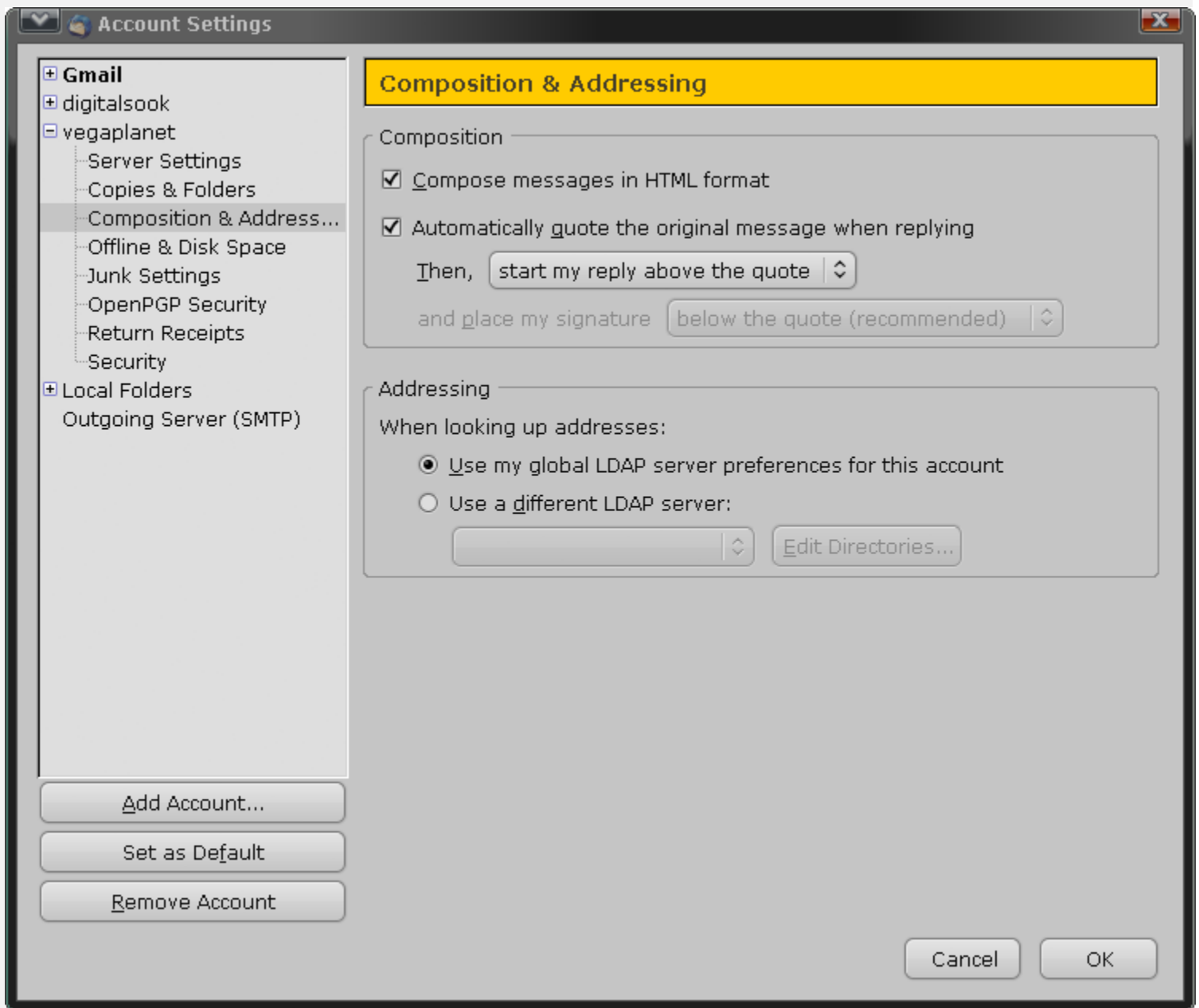
Make sure your nickname and your email address are correct here.



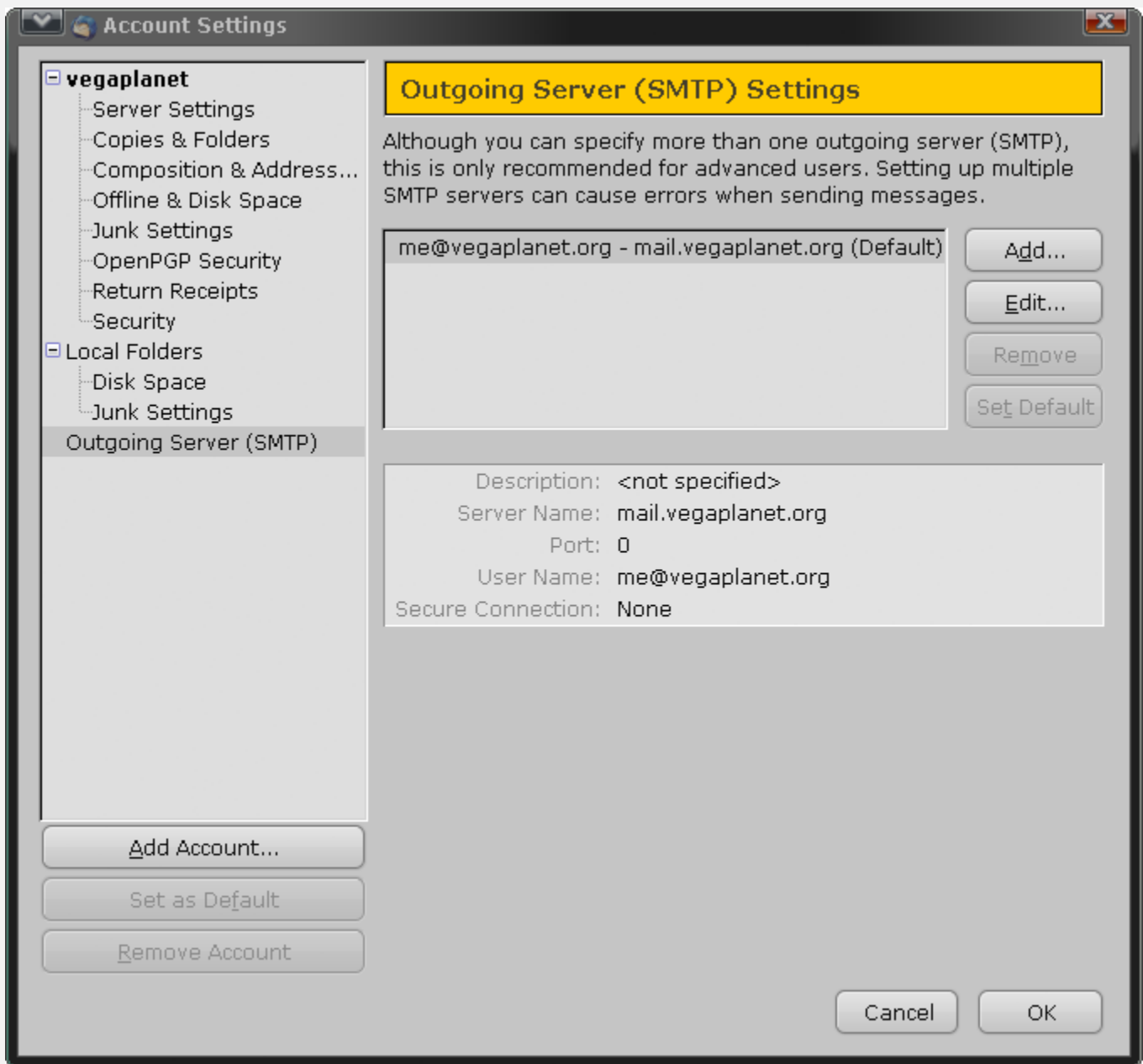
Change the **port number** to **993**,
In the "**Security settings**" options, don't forget to select "**SSL**", then make sure your config window looks like the screenshot above:



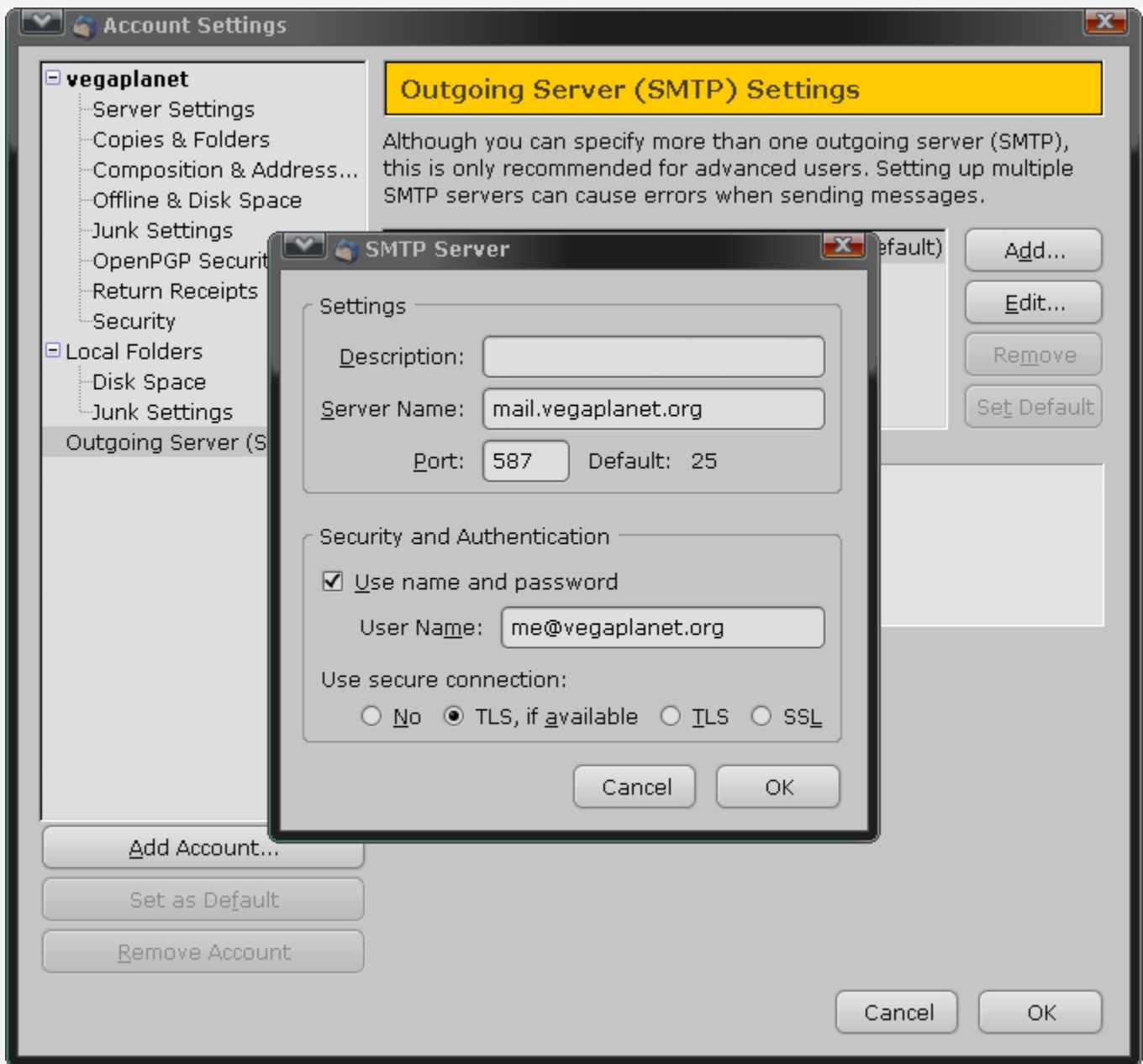
Don't forget to select the "**Place replies in the folder of the message being replied to**" option.



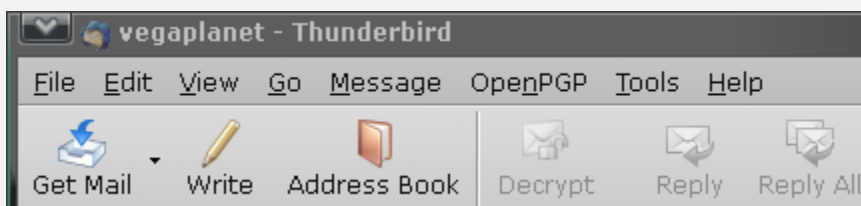
Make your configuration looks like the screenshot above:



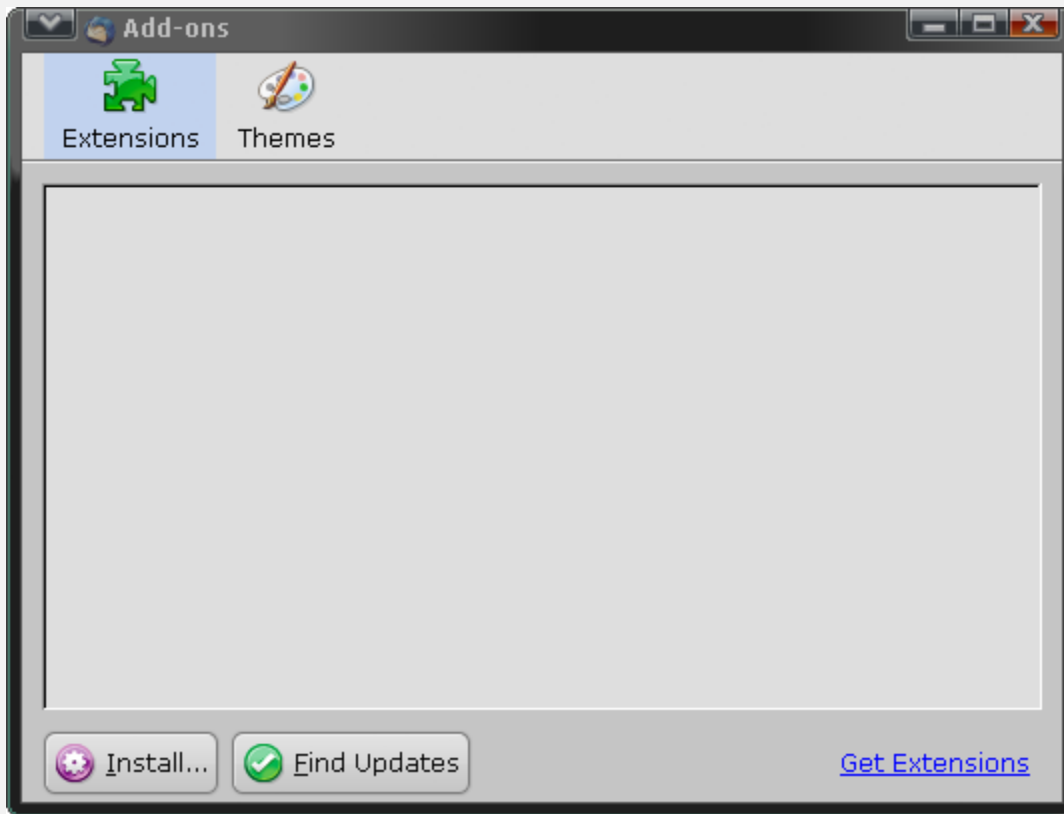
Select "**Outgoing Server (SMTP)**" in the right part of the config screen, then click on "**Edit**".



Give a description,
make sure the server name is "**mail.vegaplanet.org**",
Enter "**587**" as the **port number** (double check this, if you do it wrong, you won't be able to send any mail),
Finally select the "**TLS, if available**" option for more security, and click "**OK**"

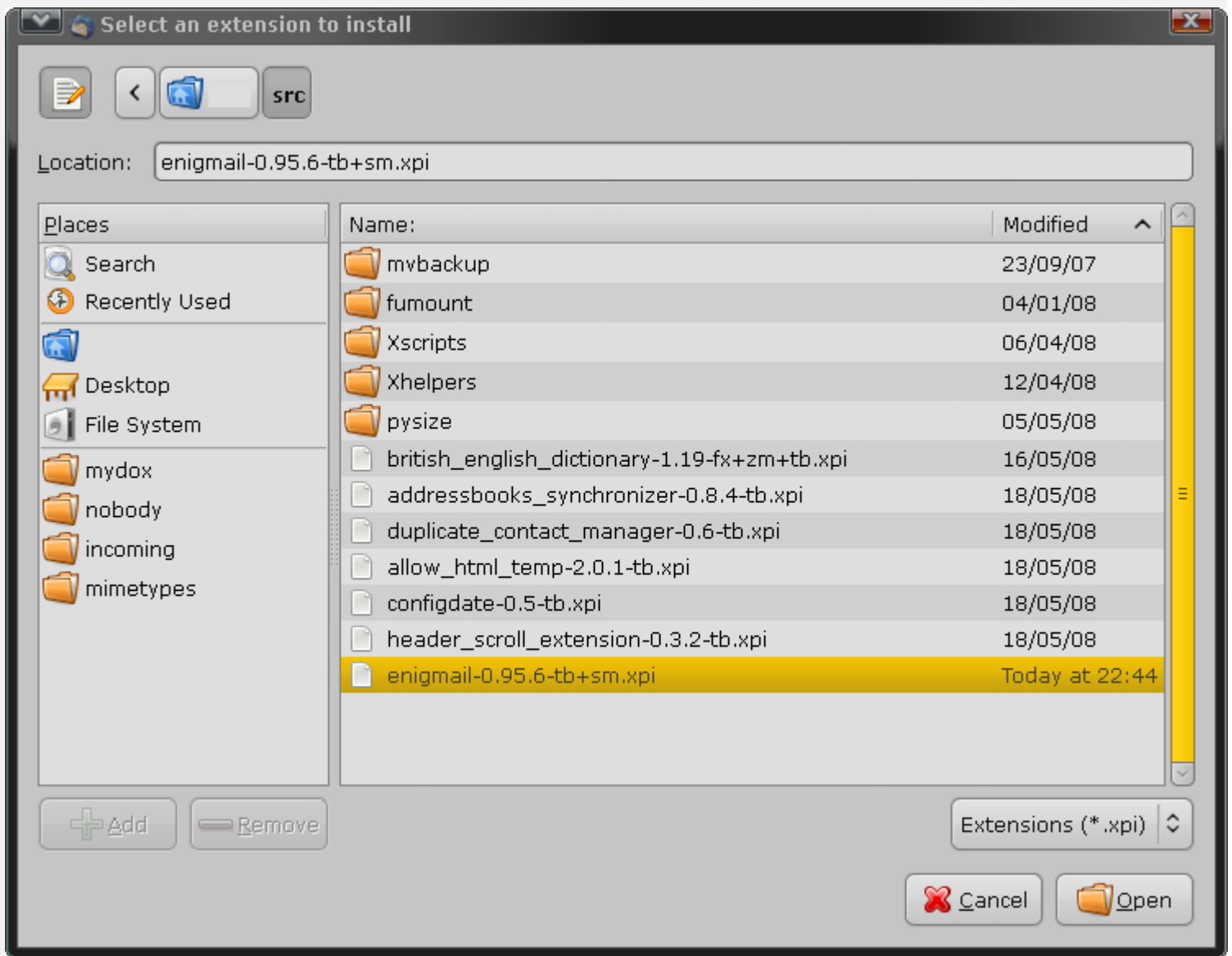


Select the "**Tools**" menu, then select the "**Add-ons**" item,



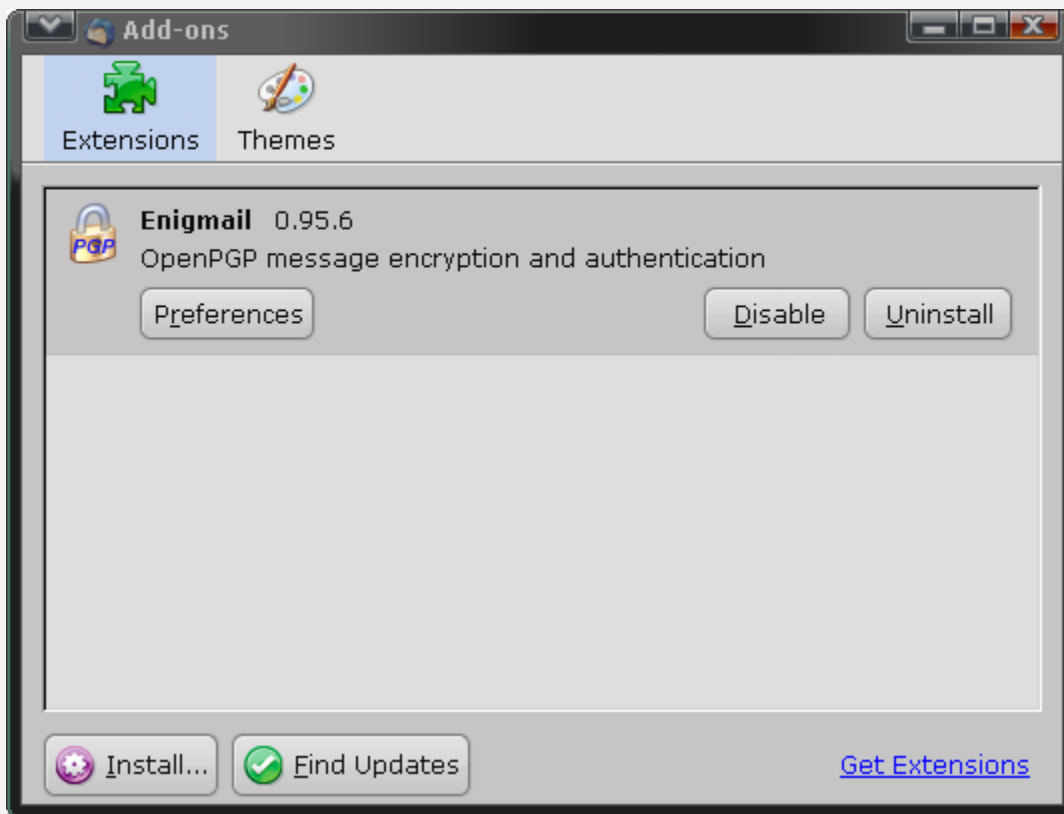
This window shows the installed plug-ins. If this is the first time you install Thunderbird, you're likely to see an empty list. Let's install the Enigmail plug-in, so click on "**Install...**"

Note: Linux users will notice Enigmail is already installed, so they can bypass the following step.



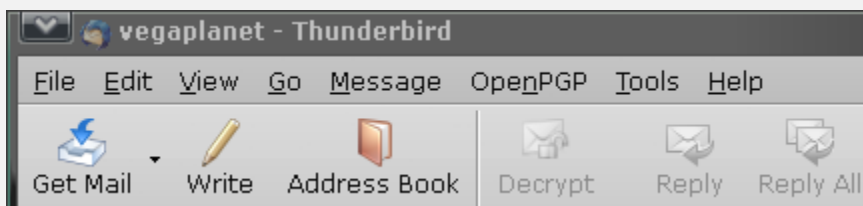
Select the Enigmail plug-in you've saved previously, then click on "Open",

Note: The file selector above may look different on your system.

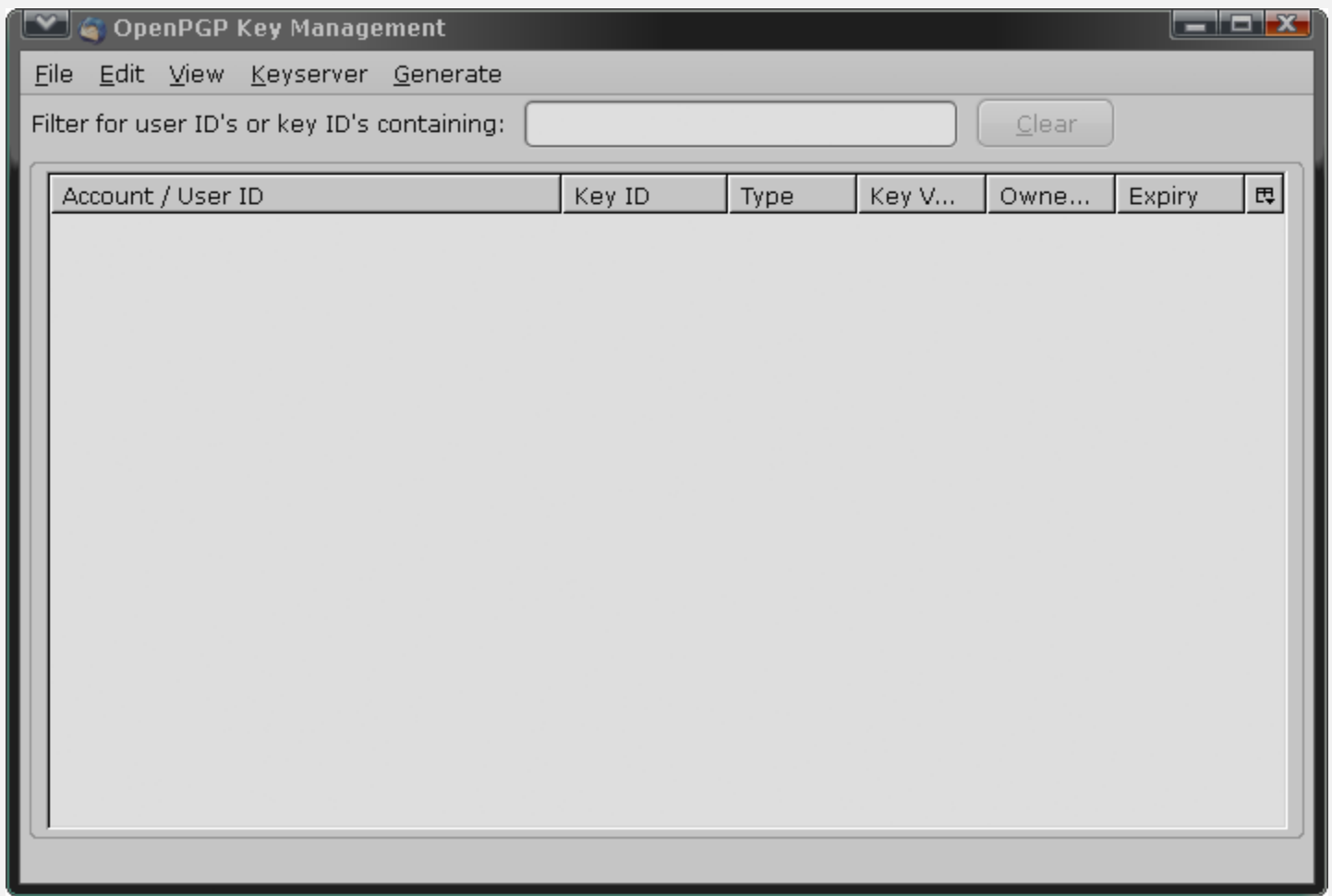


At the end your plug-in list will look like the screenshot above. You can now close this window.
Close thunderbird and restart it.

Now let's generate a new key pair!



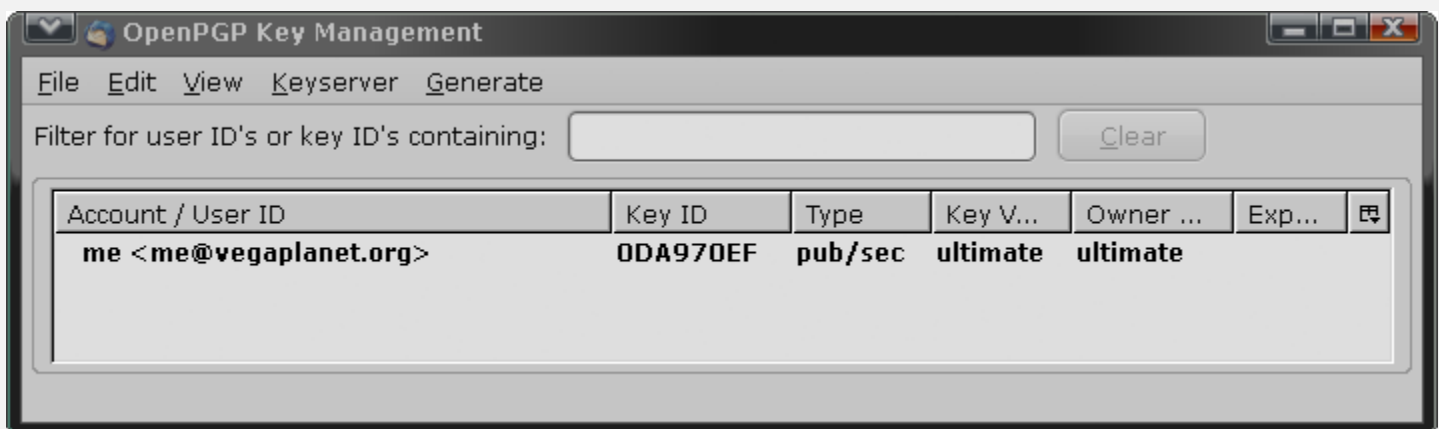
Select the "**OpenPGP**" menu and choose the "**Key management**" item.
A wizard should help you to generate your key pair. If not, or if you cancelled it accidentally, the window below will show up.



Select the **"Generate"** menu, then choose the **"New Key Pair"** item.

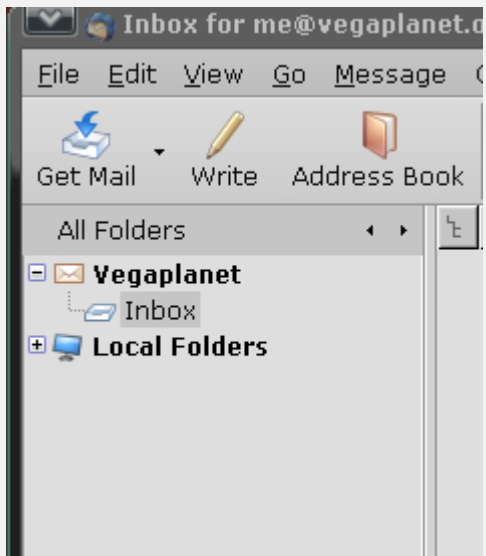


Give a passphrase for your private key (this is mandatory!),
Click on the "**Key does not expire**" option (unless you know what you're doing),
Then click on the "**Generate Key**" button,

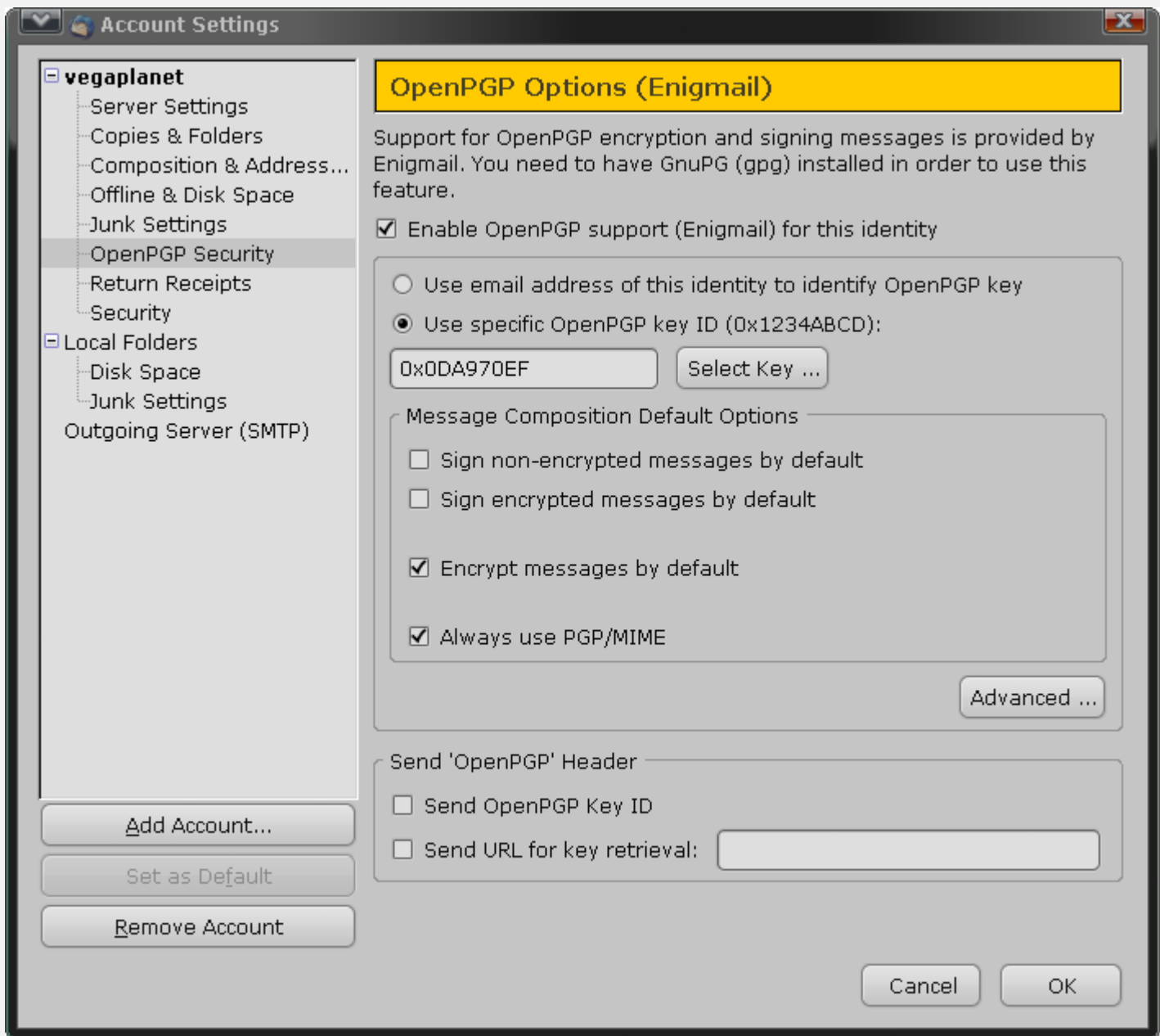


After a minute, the Key Management window will show your brand new key.

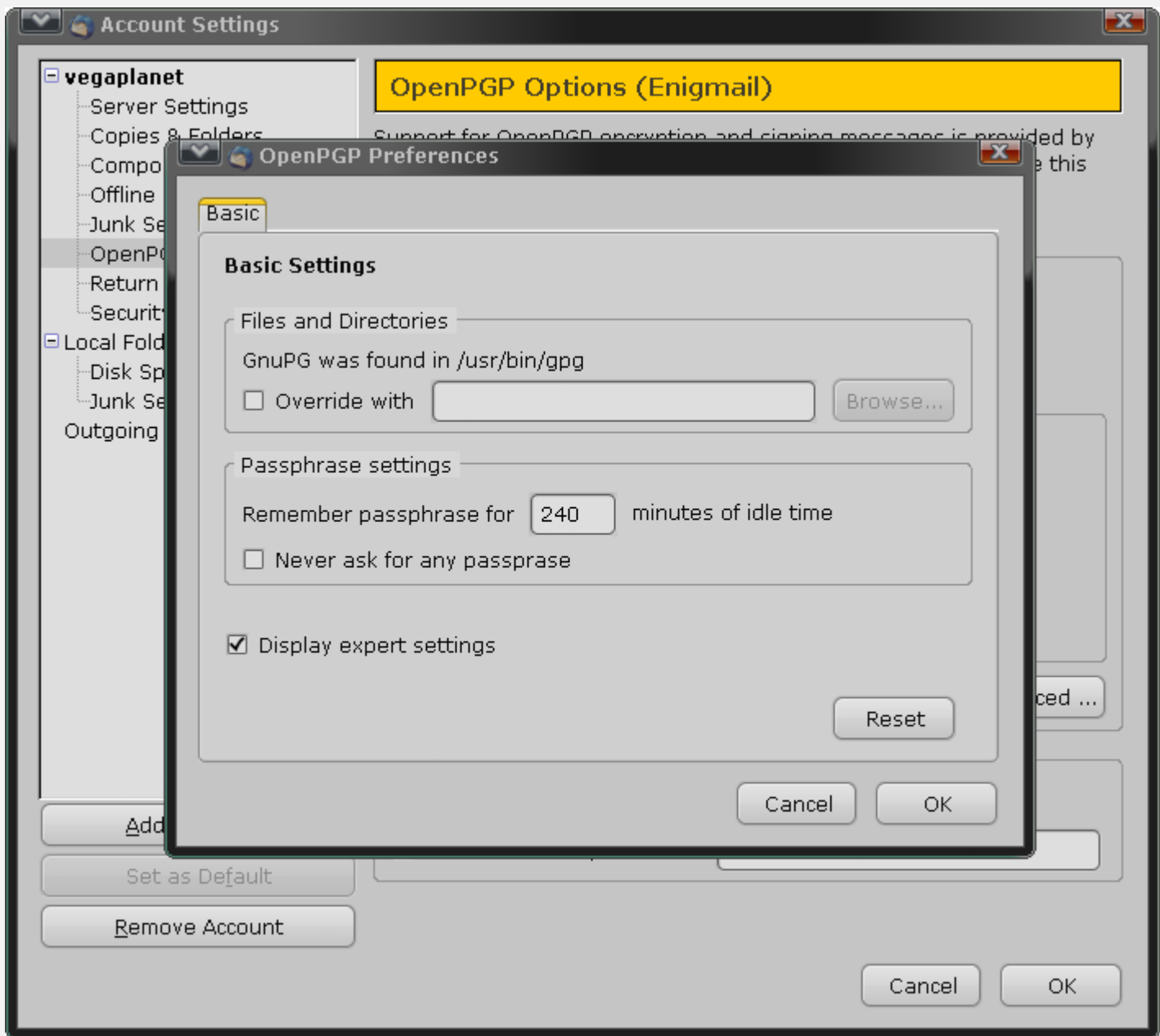
Now let's do one last config step...



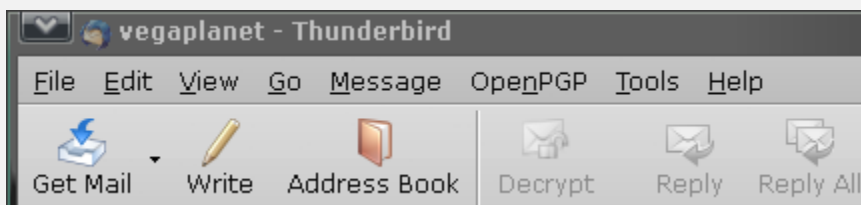
In the left part of the Thunderbird's main window, **right click on "Vegaplanet"**, select "**Properties**", then select the "**OpenPGP Security**" option.



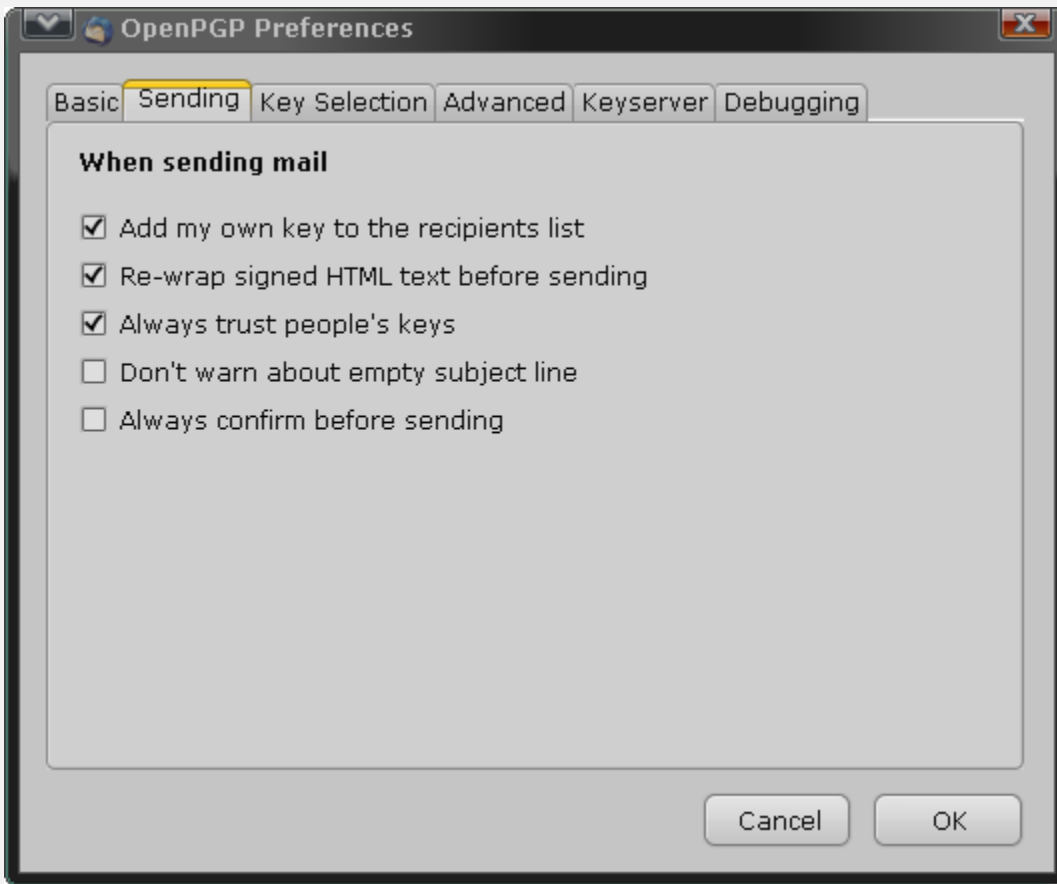
Click on "**Enable OpenPGP support**",
Click on the "**Use specific OpenPGP key ID**" option and click on the "**Select Key**" option,
Select your key when prompted,
select the "**Encrypt messages by defaults**" and "**Always use PGP/Mime**" options,
Then click on the "**Advanced**" button..



In the "**Remember passphrase**" option, choose **240** minutes (or more),
Click on the "**Display expert settings**" option, then click on "**OK**"



Select the "**OpenPGP**" menu and choose the "**Preferences**" item.



Make sure the "**Re-wrap signed HTML text before sending**" option is selected, then click on "**OK**"

That's it!

Sending & receiving encrypted emails

Importing someone's public key

You are now ready to send and receive encrypted messages. But before sending an encrypted message to your friend, you need to import his public key. The easiest way to do that is to ask your friend to send you an email with his public key. Once this is done, open your friend's message,

Select the "**OpenPGP**" menu, Select "**Sender's Key>**" and choose the "**Import public key**" option,

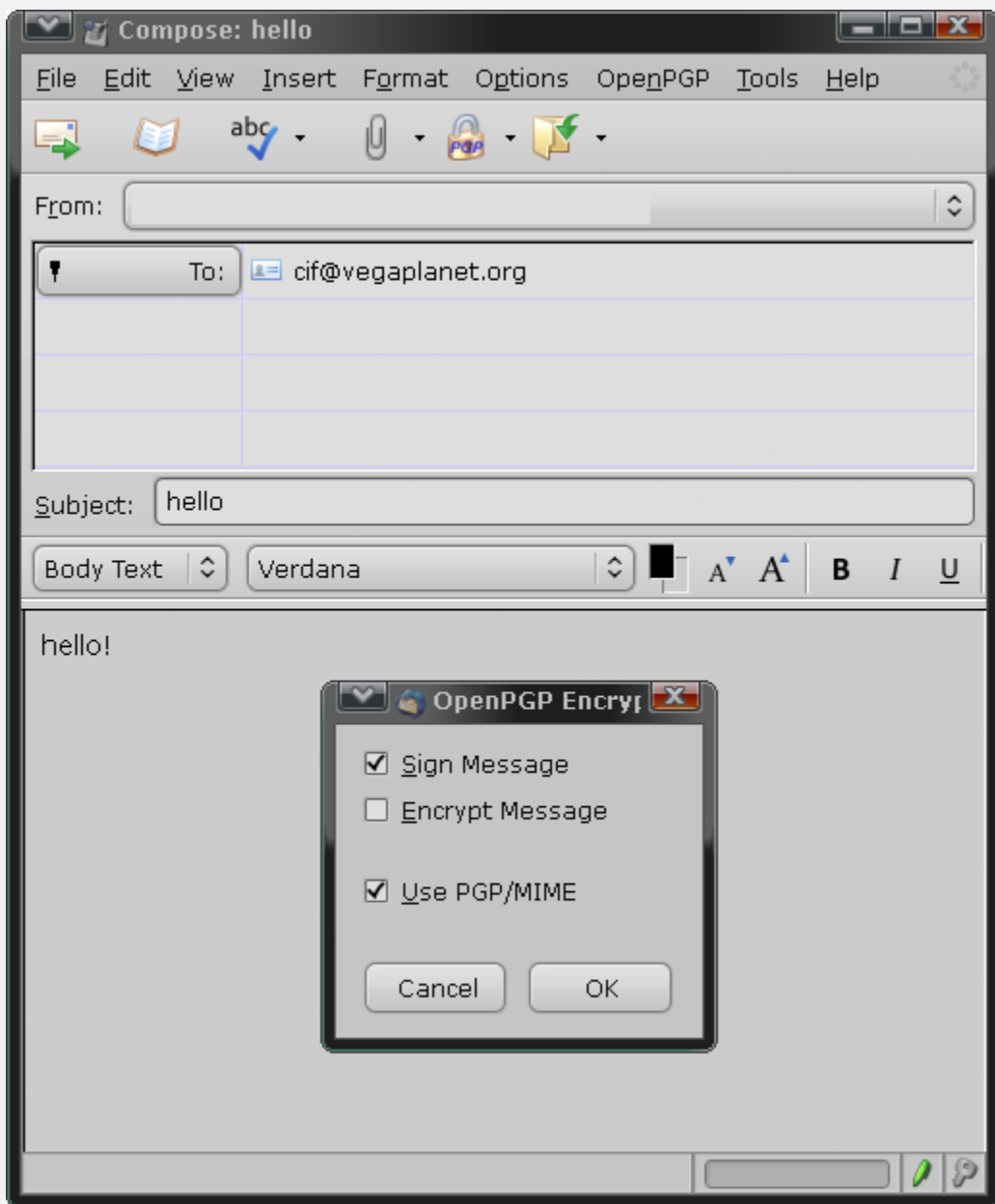
The message below will show up:



If everything goes right, you are now able to send an encrypted message to your friend. If you can't wait your friend's answer, you can also send a test email to yourself.

Sending an email

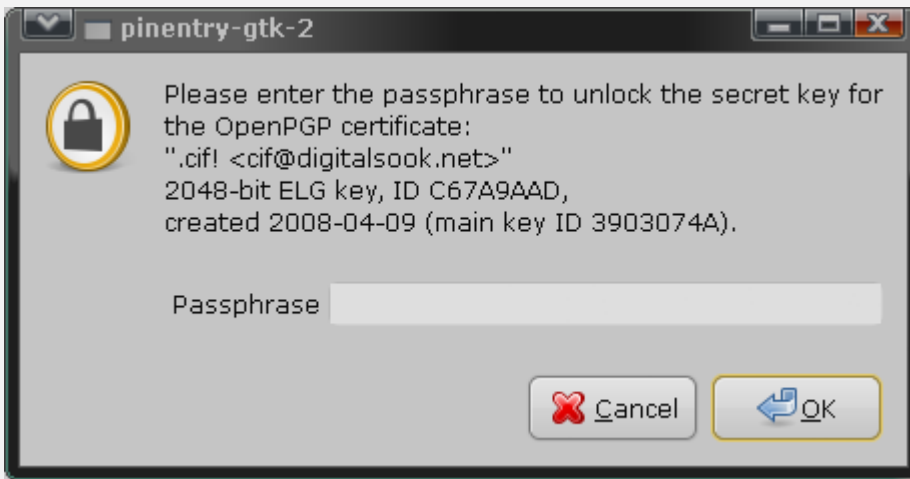
Open a new message and click on the "PGP" icon to make sure your message will be send encrypted.



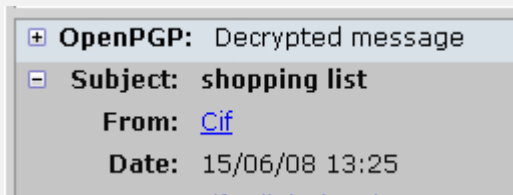
When you're done, send the message.

Receiving an encrypted email

Go to your inbox and select the message you've just received.
OpenPGP will ask you for your private key passphrase...



Give your passphrase, then click "OK"



Your message will be displayed with the text "**OpenPGP: Decrypted message**" in the mail's header.

Conclusion

Looks complicated? Not that much: In fact you'll only have to do it once and Thunderbird will encrypt and decrypt everything transparently.

If you're interested in getting a Vegaplanet email account, feel free to let me know.

In the next episode, we'll see how to chat with PGP using your regular MSN, AIM, ICQ, Google Talk account.