

How to enable email encryption on Thunderbird email client

PGP, also known as Pretty Good Privacy https://en.wikipedia.org/wiki/Pretty_Good_Privacy is a 27 years old encryption algorithm.

The system is simple. A user have 2 keys (like 2 passwords): a public key that is used to encrypt things and a private key that is used to decrypt things. So, if a user gives away his public key to anyone, then anyone can encrypt things sent to that user. The user, keeping hidden his private key and using it, is the sole person able to decrypt those things.

Such, PGP is used, amongst other things, for a system called end-to-end email encryption. The system goes like this:

- Alice has a computer, on which she runs an email client (Thunderbird) and generates a pair of keys, public and private.
- Bob has a computer, on which he runs an email client (Thunderbird) and generates a pari of keys, public and private.
- Alice send to Bob her public key, Alice keeps her private key hidden, stored safely
- Bob send to Alice his public key, Bob keeps his private key hidden, stored safely
- Alice send to Bob an email message, encrypted with Bob's public key that she has.
- Only Bob, on his own computer, where he installed the private key is able to read the message Alice sent

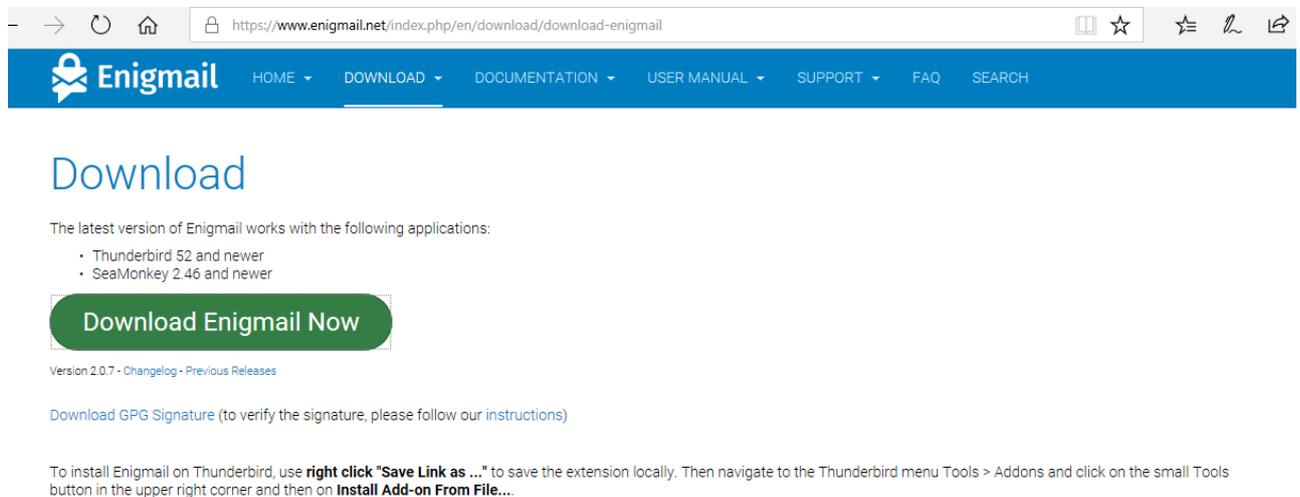
Alice and Bob can use different email clients (Thunderbird, Outlook, Mac Mail, a.s.o.) with the requirement that it supports PGP.

1. Install PGP Support on Thunderbird

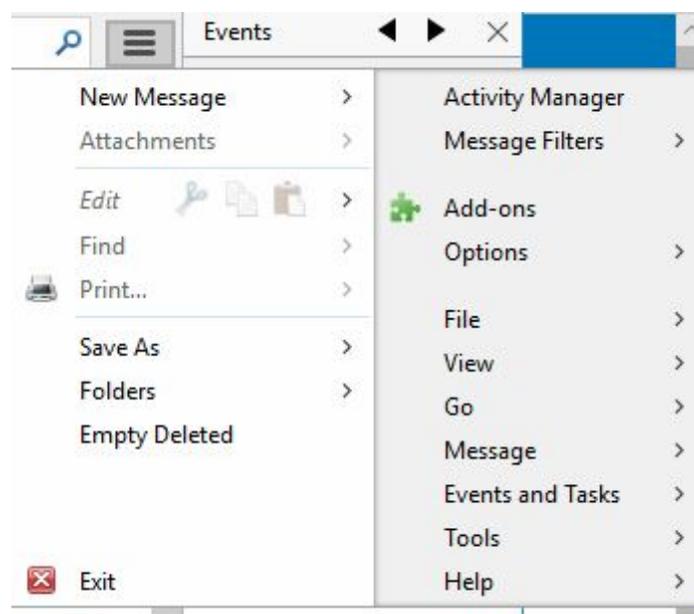
1.1. Get Enigmail Add-on

Go to <https://www.enigmail.net/index.php/en/download/download-enigmail>

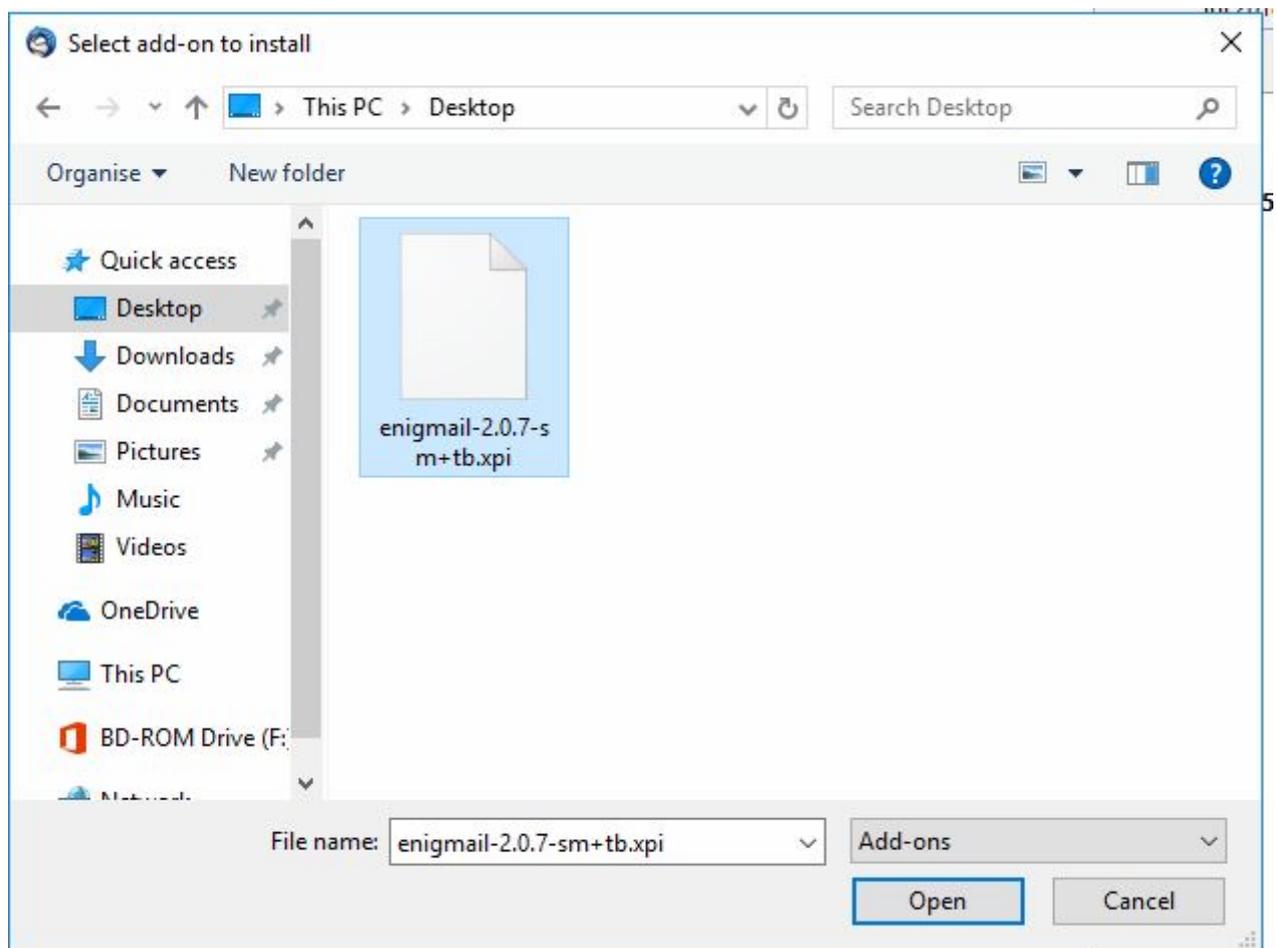
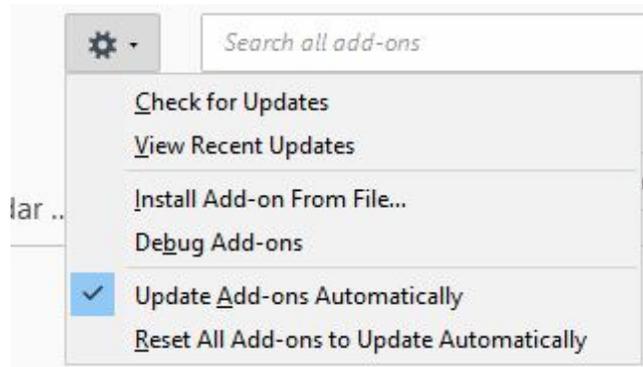
Click "Download Enigmail Now"

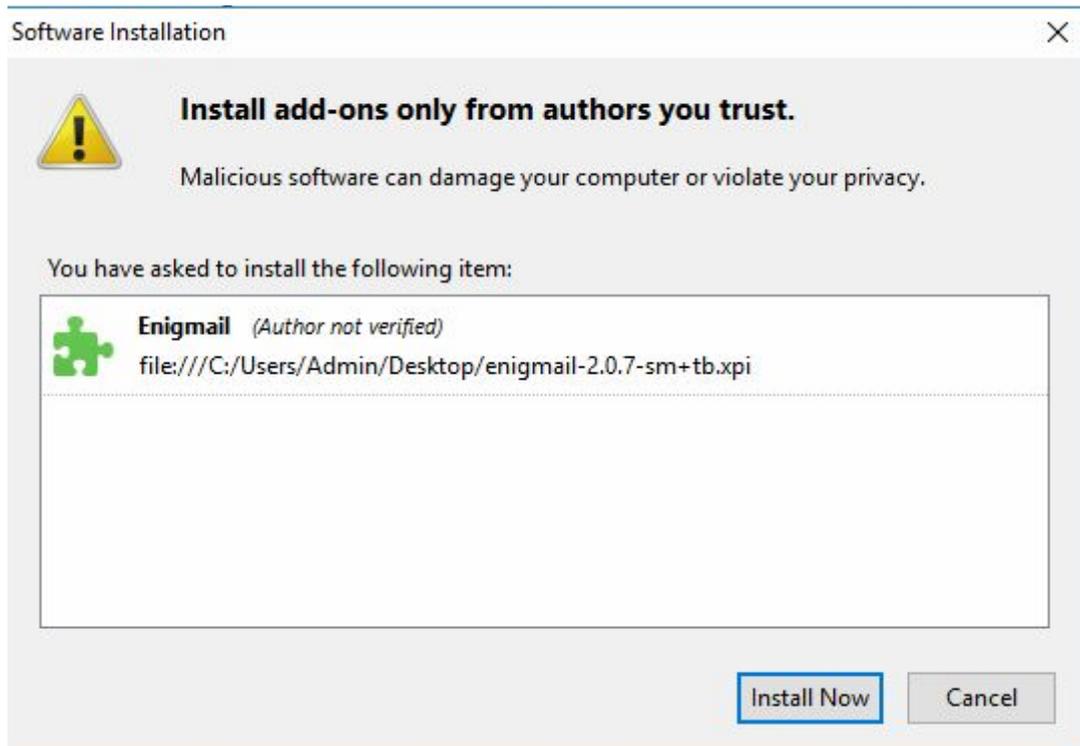


1.2. After the file is downloaded select Thunderbird Menu -> Add-ons

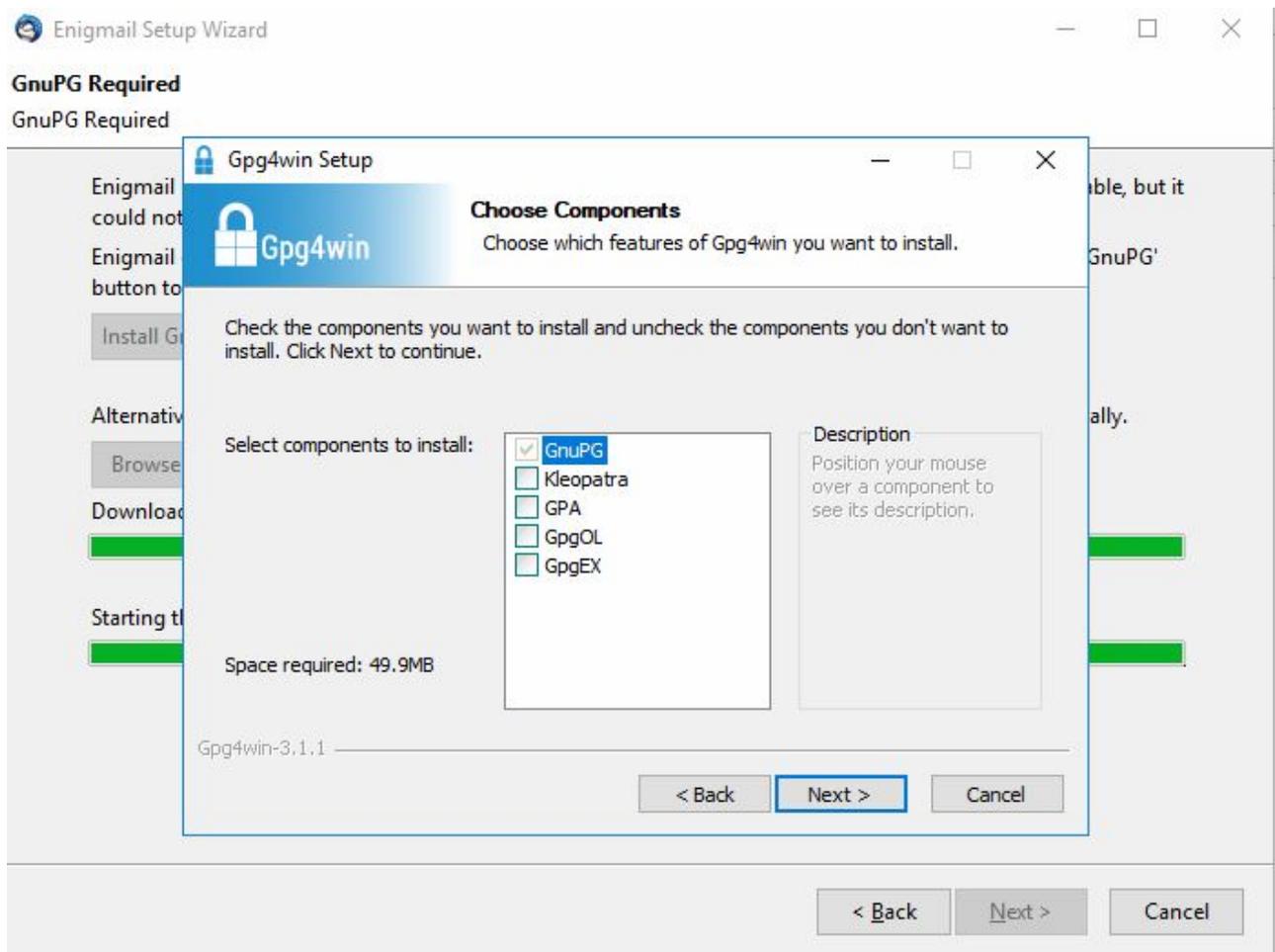
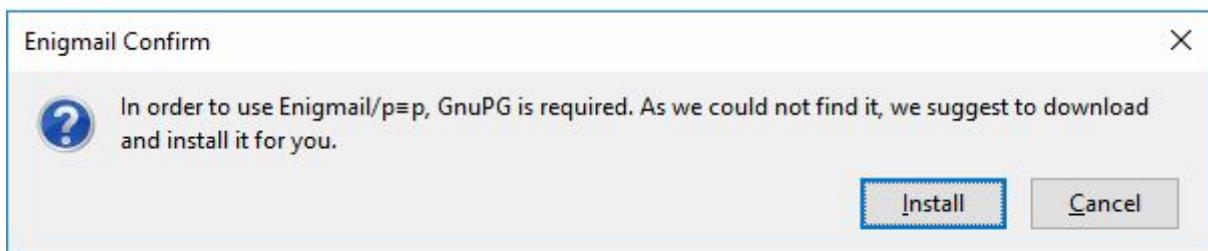
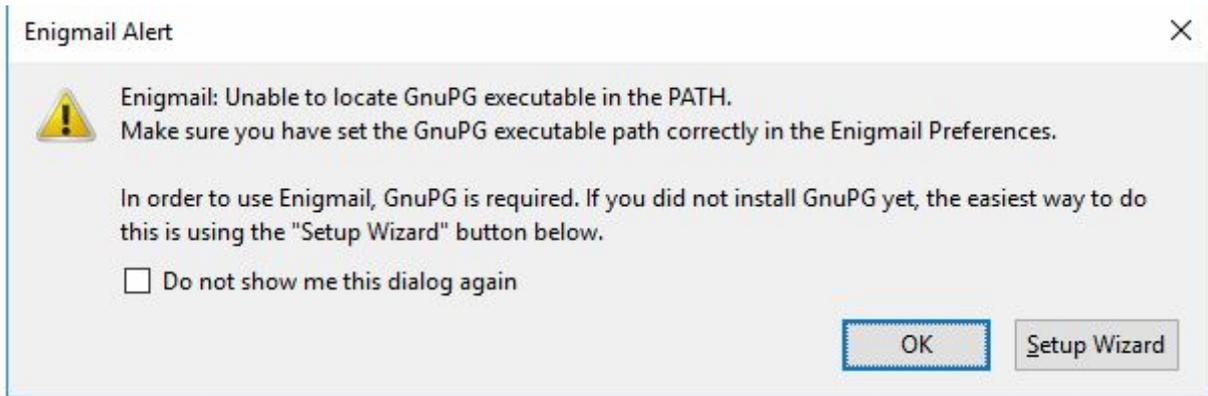


1.3. Next select "Tools for all add-ons" -> Install Add-on From File..".

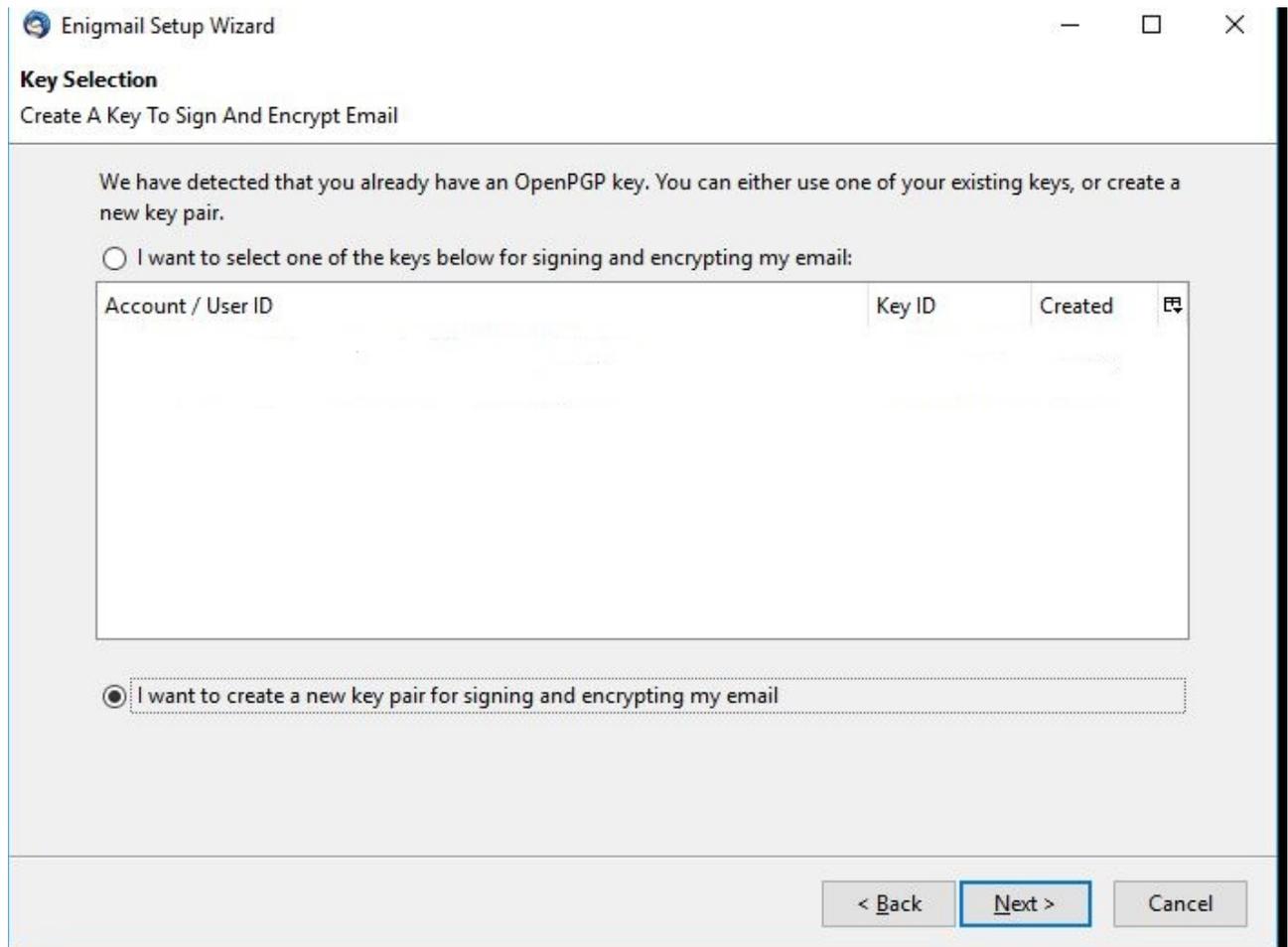




1.4. Click OK -> Install



1.5. Select " I want to create a new key pair for signing and encrypting my email" -> Click Next



1.6. Enter a passphrase -> Click Next

The screenshot shows the 'Enigmail Setup Wizard' window, specifically the 'Create Key' step. The window title is 'Enigmail Setup Wizard' and it has standard window controls (minimize, maximize, close). The main heading is 'Create Key' with the subtitle 'Create a new Key Pair'. The text explains that the dialog will create a pair of keys: a public key for others to send encrypted emails, and a secret key for the user to decrypt and sign emails. It also explains the purpose of a passphrase to protect the secret key, noting it should be at least 8 characters and include digits and punctuation, but avoid umlauts and language-specific characters. The 'Account / User ID' is listed as 'Valentin Besleaga <valentin.besleaga@camscape.ro> - valentin.besleaga@camscape.ro'. There are two input fields for the passphrase, both filled with dots. Below them is a 'Passphrase quality' indicator, which is a green bar. At the bottom, there is a dropdown menu for 'Remember passphrase for' set to '10' minutes. The 'Next >' button is highlighted with a blue border, indicating it is the next step to take.

Enigmail Setup Wizard

Create Key

Create a new Key Pair

This dialog will create a pair of keys:

Your **public key** is **for others** to send you encrypted emails. You can distribute it to everybody.

Your **secret key** is **for you** to decrypt these emails and to send signed emails. You should give it to nobody.

Your **passphrase** is a password to protect your secret key. It prevents misuse of your secret key. The passphrase should contain several words and at least 8 characters, digits and punctuation marks. Umlauts (e.g. ä, é, ñ) and language-specific characters are **not** recommended.

Account / User ID:
Valentin Besleaga <valentin.besleaga@camscape.ro> - valentin.besleaga@camscape.ro

Passphrase
●●●●●●●●

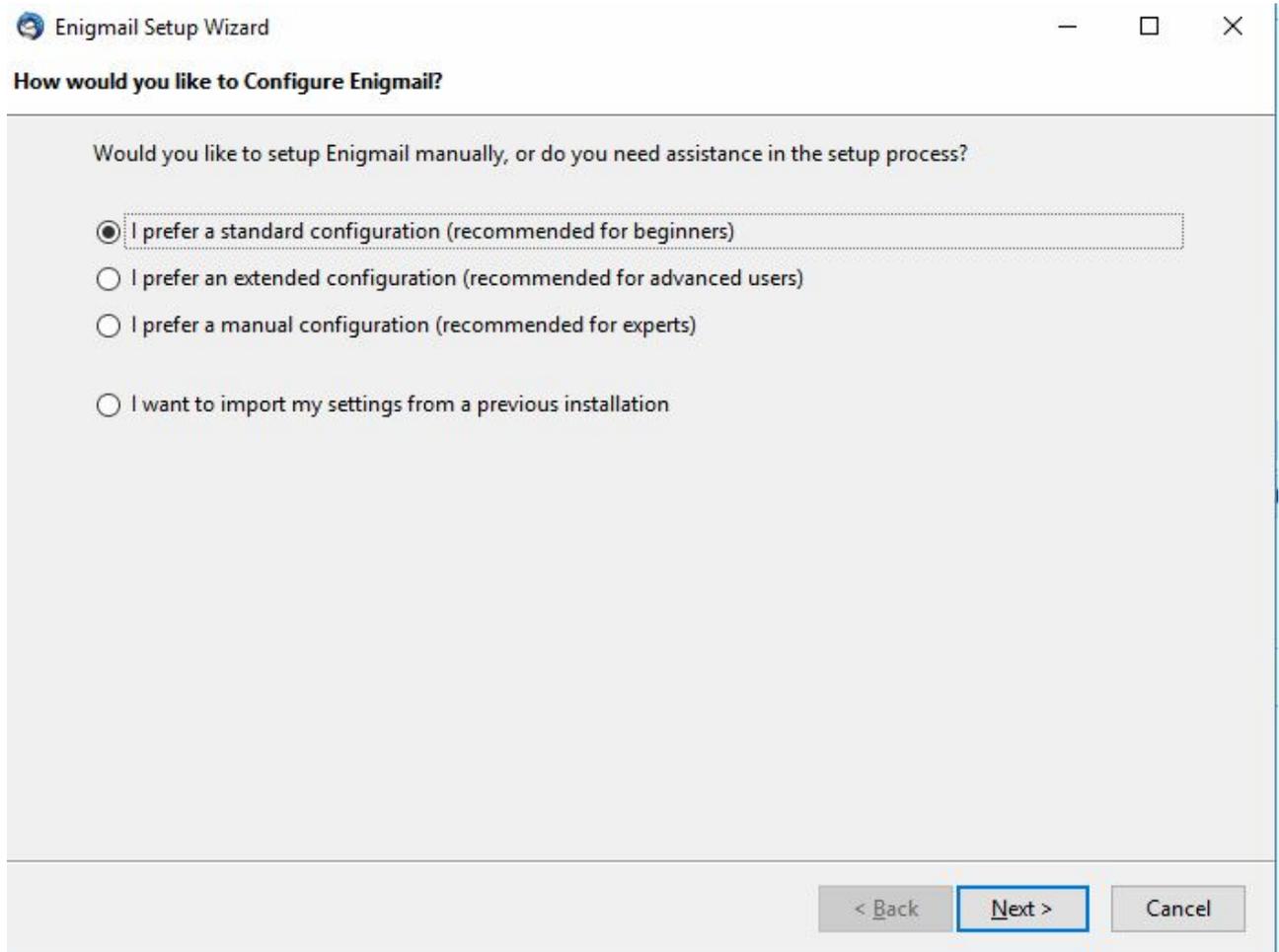
Please confirm your passphrase by typing it again
●●●●●●●●

Passphrase quality:
■■■■■■■■■■

Remember passphrase for 10 minutes of inactivity (before needing to re-enter it)

< Back Next > Cancel

1.7. Select "I prefer a standard configuration (recommended for beginners)" -> Click Next



Enigmail Setup Wizard

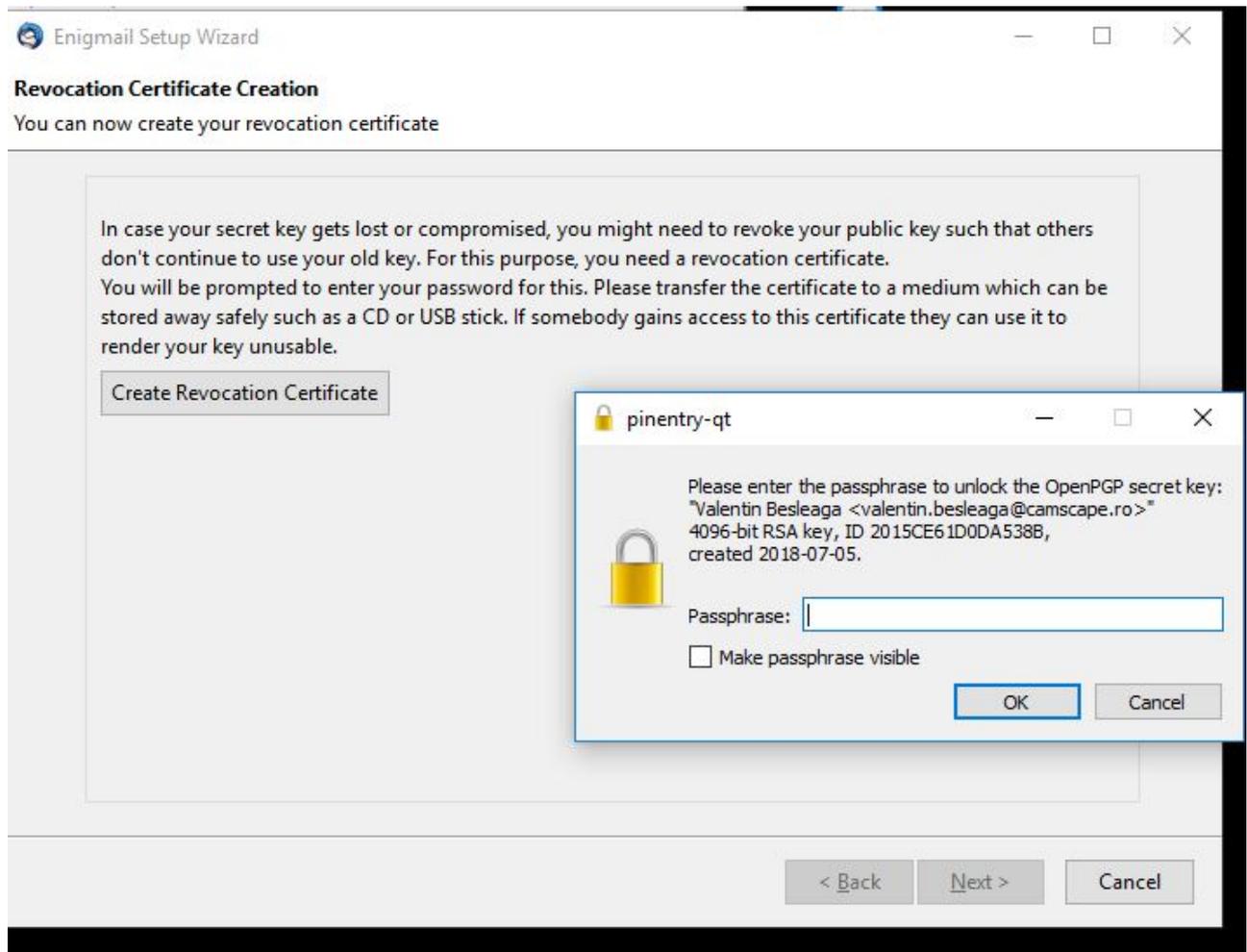
How would you like to Configure Enigmail?

Would you like to setup Enigmail manually, or do you need assistance in the setup process?

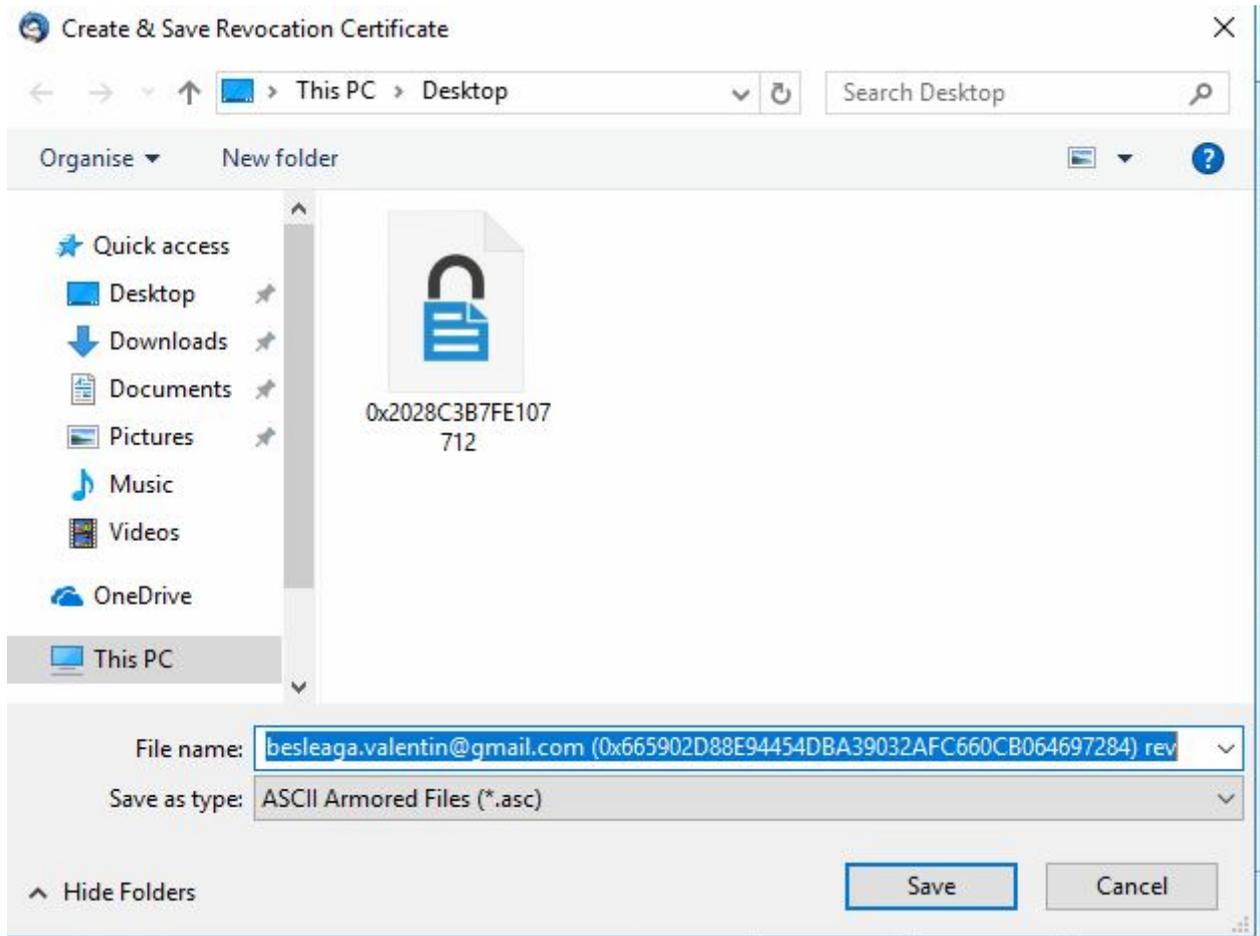
- I prefer a standard configuration (recommended for beginners)
- I prefer an extended configuration (recommended for advanced users)
- I prefer a manual configuration (recommended for experts)
- I want to import my settings from a previous installation

< Back Next > Cancel

1.8. Select "Create Revocation Certificate" -> Enter the passphrase entered earlier -> Click OK

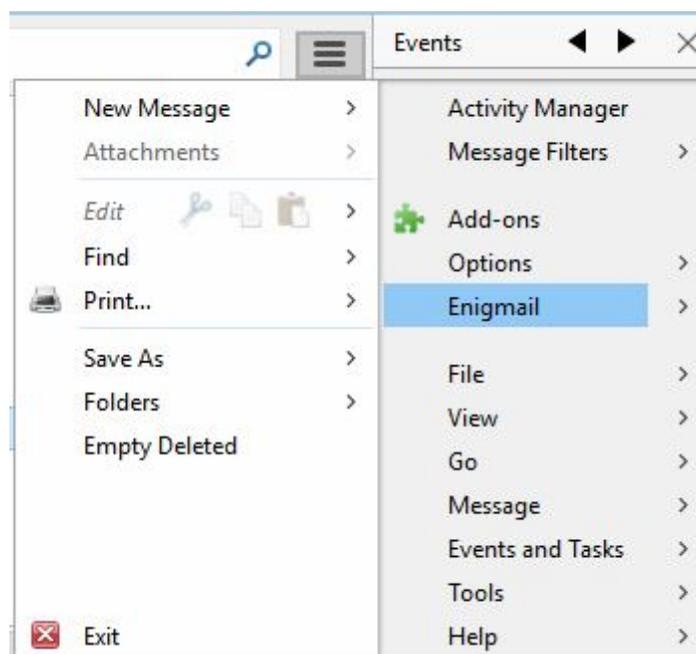


1.9. Save the revocation certificate. Recommended to another device (USB flash drive, External HDD)

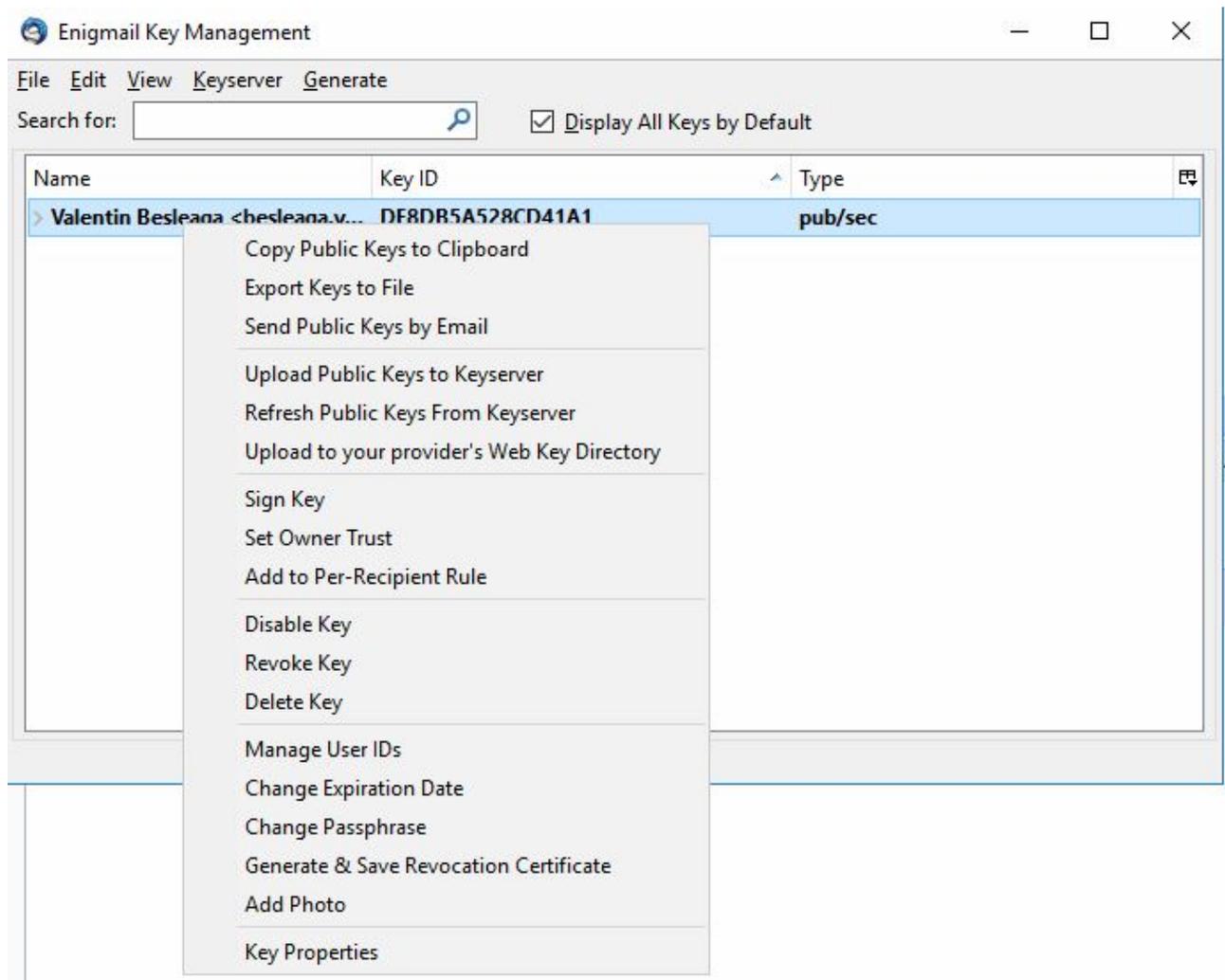


2. Start sending encrypted email

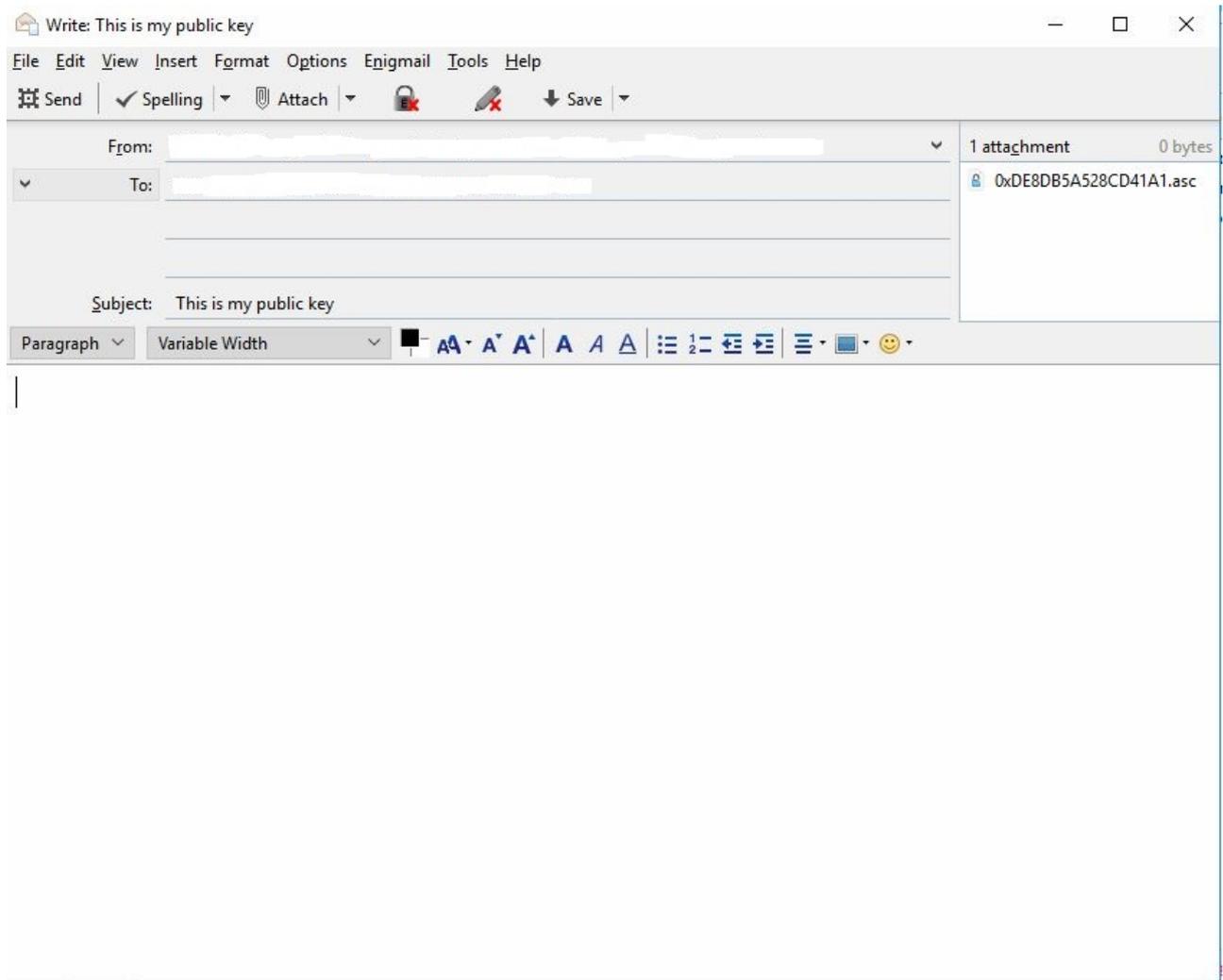
2.1. From Thunderbird Menu , select Enigmail -> Key Management



2.2. Right click on the key created earlier -> Select "Send Public Key by email"

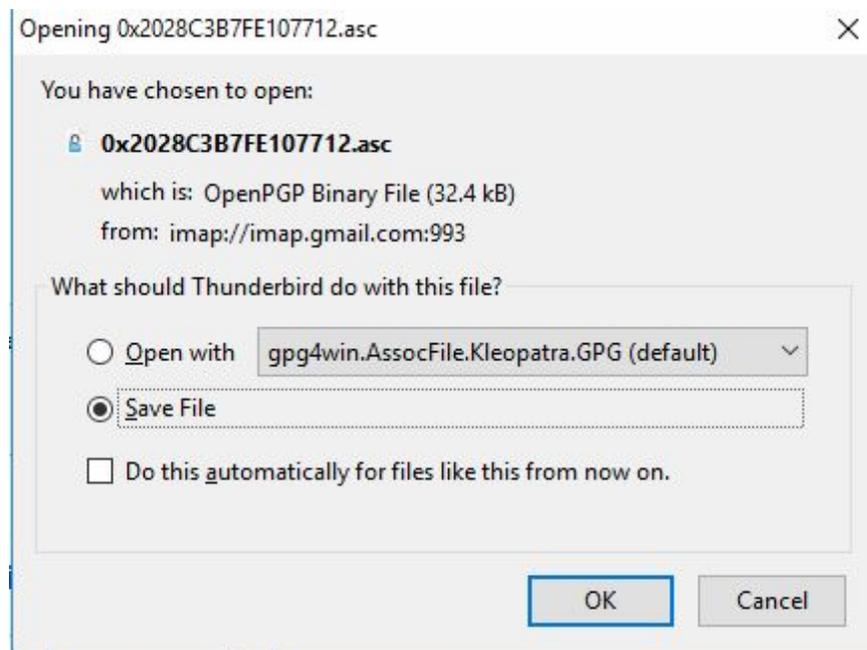


2.3. Send the public key to the receiver

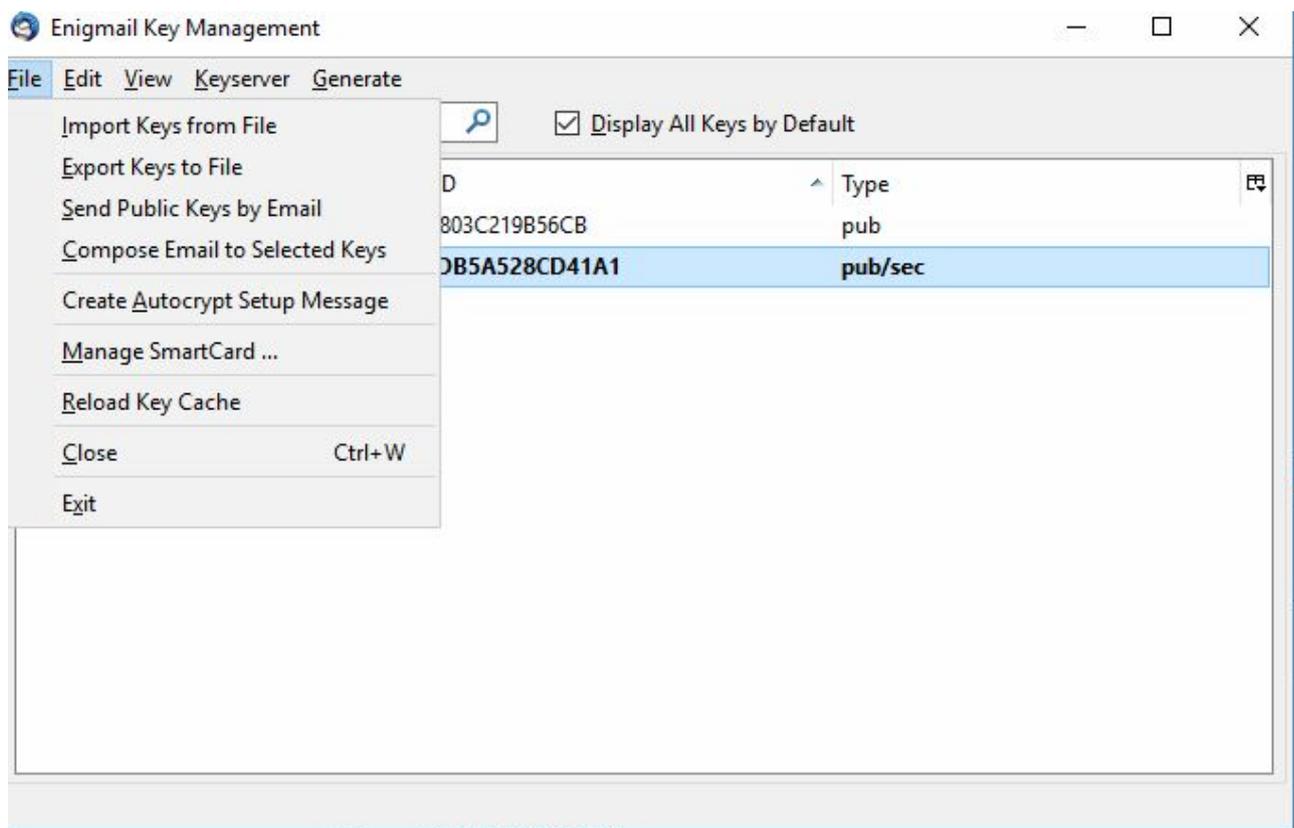


2.4. Save the public key file.

The public key that was send to you by the future recipient, using the same procedure as above, must be saved first locally before use.



2.5. From Thunderbird Menu -> Enigmail -> Key Management, select File -> Import Keys from file.



3. Send PGP encrypted email

Having your public key sent to the final recipient and his public key imported into Thunderbird, you can now send an encrypted email that only him can read.

Write a new email, and check if the marked buttons are shown as bellow, then enter the passphrase you entered earlier.

