

# How to enable email encryption on Thunderbird email client

PGP, also known as Pretty Good Privacy <u>https://en.wikipedia.org/wiki/Pretty\_Good\_Privacy</u> 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.



#### **<u>1. Install PGP Support on Thunderbird</u>**

#### 1.1. Get Enigmail Add-on

#### Go to <u>https://www.enigmail.net/index.php/en/download/download-enigmail</u> Click "Download Enigmail Now"

	□ ☆	∑≞	l~	Ŀ
Enigmail Home - download - documentation - user manual - support - FAQ SEARCH				
Download				
The latest version of Enigmail works with the following applications: <ul> <li>Thunderbird 52 and newer</li> <li>SeaMonkey 2.46 and newer</li> </ul>				
Download Enigmail Now				
Version 2.0.7 - Changelog - Previous Releases				
Download GPG Signature (to verify the signature, please follow our instructions)				
To install Enigmail on Thunderbird, use <b>right click "Save Link as</b> " to save the extension locally. Then navigate to the Thunderbird menu Tools > Addons button in the upper right corner and then on Install Add-on From File	and click on the :	small To	ols	

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





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



→ Y 小 いい PC > Desktop	S ~	Search Desktop	م ر
Organise 🔻 New folder			- 💷 🤅
<ul> <li>Quick access</li> <li>Desktop</li> <li>Downloads</li> <li>Documents</li> <li>Pictures</li> <li>Pictures</li> <li>Music</li> <li>Videos</li> <li>OneDrive</li> <li>This PC</li> <li>BD-ROM Drive (F:</li> </ul>			
File name: enigmail-2.0.7-sm+	-tb.xpi ~	Add-ons	~



Install add-ons only from authors you trust. Malicious software can damage your computer or violate your privacy.      ou have asked to install the following item:     Enigmail (Author not verified)     file:///C:/Users/Admin/Desktop/enigmail-2.0.7-sm+tb.xpi	
ou have asked to install the following item: Enigmail (Author not verified) file:///C:/Users/Admin/Desktop/enigmail-2.0.7-sm+tb.xpi	
Enigmail (Author not verified) file:///C:/Users/Admin/Desktop/enigmail-2.0.7-sm+tb.xpi	
file:///C:/Users/Admin/Desktop/enigmail-2.0.7-sm+tb.xpi	
Install Now Canc	el



#### 1.4. Click OK -> Install





	Gpg4win Setup		– 🗆 🗙	
Enigmail could not Enigmail	Gpg4win	Choose Components Choose which features	of Gpg4win you want to install.	ible, but it GnuPG'
Install G	Check the component install. Click Next to co	s you want to install and uncheo Intinue.	ck the components you don't want to	
Alternativ	Select components to		Description	a <mark>lly.</mark>
Browse	Select components to	Kleopatra	Position your mouse over a component to	
Download		GPA GpgOL GpgEX	see its description.	
Starting t				
	Space required: 49.9N	18		
	Gpg4win-3,1,1	<u>.</u>		
		<	Back Next > Cancel	



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

Ne have detected that you already have an Open	PGP key. You can either use one of your exis	ting keys, or cre	ate a
<ul> <li>I want to select one of the keys below for sign</li> </ul>	ning and encrypting my email:		
Account / User ID	Key ID	Created	E
I want to create a new key pair for signing and	d encrypting my email		
I want to create a new key pair for signing and	d encrypting my email		



### <u>1.6. Enter a passphase -> Click Next</u>

Enigmail Setup Wizard	72_35		×
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 t	o nobody	у.	
Your <b>passphrase</b> is a password to protect your secret key. It prevents misuse of your secret key. Th should contain several words and at least 8 characters, digits and punctuation marks. Umlauts (e. language-specific characters are <b>not</b> recommended.	ne passph g. ä, é, ñ)	and	
Account / User ID: Valentin Besleaga <valentin.besleaga@camscape.ro> - 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)		~	
< <u>B</u> ack <u>N</u> e	xt >	Cance	:
		1	



### 1.7. Select "I prefer a standard configuration (recommened 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)			
<ul> <li>I prefer an extended configuration (recommended for advanced users)</li> </ul>			
<ul> <li>I prefer a manual configuration (recommended for experts)</li> </ul>			
<ul> <li>I want to import my settings from a previous installation</li> </ul>			
Pack N	ent >	Can	al
< Dack	CAL >	Cano	



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

evocation Certificate Creation ou can now create your revocation certificate				
In case your secret key gets lost or compromis don't continue to use your old key. For this pu You will be prompted to enter your password stored away safely such as a CD or USB stick. It render your key unusable.	ed, you might need to revoke your public k rpose, you need a revocation certificate. for this. Please transfer the certificate to a m f somebody gains access to this certificate t	ey such that oth nedium which ca hey can use it to	ners an be	
Create Revocation Certificate	<ul> <li>pinentry-qt</li> <li>Please enter the passphras Valentin Besleaga <valenti 4096-bit RSA key, ID 20150 created 2018-07-05.</valenti </li> <li>Passphrase:</li> <li>Make passphrase visible</li> </ul>	e to unlock the O n.besleaga@cam CE6 1D0DA538B,	penPGP secr scape.ro>"	> et ke
1.		OK	Can	cel



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

	22 2 2 2	10221		
$\rightarrow$ $\checkmark$ $\uparrow$ $\square$ $\rightarrow$ This	PC > Desktop	~ Q	Search Desktop	Q
Organise 🔻 🛛 New folder				• 0
<ul> <li>▲</li> <li>▲</li> <li>▲</li> <li>▲</li> <li>Desktop</li> <li>▲</li> <li>Downloads</li> <li>▲</li> <li>■</li> <li>Documents</li> <li>▲</li> <li>▲</li> <li>■</li> <li>Pictures</li> <li>★</li> <li>▲</li> <li>Music</li> <li>■</li> <li>Videos</li> <li>▲</li> <li>OneDrive</li> </ul>	0x2028C3B7FE107 712			
This PC				
File name: besleag	ga.valentin@gmail.com (0x	665902D88E94454D	BA39032AFC660CB064697	284) rev
Save as type: ASCII A	rmored Files (*.asc)			



2. Start sending encrypted email

#### • • Events × م = New Message > Activity Manager Attachments Message Filters ÿ > So. Edit B. 1 > **2** Add-ons Find > Options > A Print... > Enigmail > Save As > File > Folders > View 5 Empty Deleted Go > Message > **Events and Tasks** > Tools > 🔀 Exit Help >

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



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

K C I					
Keyserver Generate	by Defa	ult			
Key ID	~	Туре			C,
Ana besleana.v DF8DR5A528CD41A1 Copy Public Keys to Clipboard Export Keys to File Send Public Keys by Email Upload Public Keys to Keyserver Refresh Public Keys From Keyserver Upload to your provider's Web Key Directory Sign Key Set Owner Trust Add to Per-Recipient Rule Disable Key Revoke Key Delete Key		pub/sec			
Manage User IDs Change Expiration Date Change Passphrase Generate & Save Revocation Certificate Add Photo					
	Keyserver       Generate         Key ID         ana <besteana.v< td="">       DF8DB5A528CD41A1         Copy Public Keys to Clipboard         Export Keys to File         Send Public Keys to Keyserver         Refresh Public Keys to Keyserver         Refresh Public Keys Trom Keyserver         Upload to your provider's Web Key Directory         Sign Key         Set Owner Trust         Add to Per-Recipient Rule         Disable Key         Revoke Key         Delete Key         Manage User IDs         Change Expiration Date         Change Passphrase         Generate &amp; Save Revocation Certificate         Add Photo</besteana.v<>	Keyserver       Generate         Rey ID       Ana <bedeana.v< td="">         ana <bedeana.v< td="">       DF8DB5A528CD41A1         Copy Public Keys to Clipboard       Export Keys to File         Send Public Keys to Keyserver       Send Public Keys to Keyserver         Upload Public Keys to Keyserver       Upload to your provider's Web Key Directory         Sign Key       Set Owner Trust         Add to Per-Recipient Rule       Disable Key         Delete Key       Manage User IDs         Change Expiration Date       Change Passphrase         Generate &amp; Save Revocation Certificate       Add Photo</bedeana.v<></bedeana.v<>	Keysserver       Generate         Key ID       Type         ana chesleana.v       DF8DB5A528CD41A1       pub/sec         Copy Public Keys to Clipboard       Export Keys to File       pub/sec         Send Public Keys to File       Send Public Keys to Keyserver       Public Keys to Keyserver         Upload Public Keys to Keyserver       Upload to your provider's Web Key Directory       Sign Key         Set Owner Trust       Add to Per-Recipient Rule       Disable Key         Disable Key       Revoke Key       Delete Key         Manage User IDs       Change Expiration Date       Change Passphrase         Generate & Save Revocation Certificate       Add Photo       Image User IDs	Keyserver       Desplay All Keys by Default         Key ID       Type         ana < bedeana.v	Keyserver       Desplay All Keys by Default         Key ID       Type         ana checkeana.v       DF8DR5A528CD41A1       pub/sec         Copy Public Keys to Clipboard       Export Keys to File       pub/sec         Send Public Keys to File       Send Public Keys to Keyserver       pub/sec         Refresh Public Keys to Keyserver       Refresh Public Keys to Keyserver       pub/sec         Vpload to your provider's Web Key Directory       Sign Key       Set Owner Trust         Add to Per-Recipient Rule       Disable Key       publet Key         Disable Key       Revoke Key       pelete Key         Manage User IDs       Change Expiration Date       Change Passphrase         Generate & Save Revocation Certificate       Add Photo       Image Content Certificate



for excellent IT solutions

## 2.3. Send the public key to the receiver

Send ,	Spelling -	🛛 🛛 Attach	- 🔒	R	<b>↓</b> Save	•					
F <u>r</u>	om:								v	1 atta <u>c</u> hment	0 byte
~	To:									OxDE8DB5A528	CD41A1.asc
	·										
<u>S</u> ubj	ect: This is	my public key	N.I.						_		
Paragraph 🗸	Variable V	Vidth	~ =-	A . A . A	AA		0 0 E	• 🔳 • 🙂	•		



# 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.

0	pening 0x2028C3B7F	E107712.asc	×
,	You hav <mark>e chosen to</mark>	open:	
	■ 0x2028C3B7F	E107712.asc	
	which is: Oper	nPGP Binary File (32.4 kB)	
	from: imap://	imap.gmail.com:993	
	What should Thun	derbird do with this file?	
	O Open with	gpg4win.AssocFile.Kleopatra.GPG (default) ×	
	Save File		
	Do this <u>a</u> uto	matically for files like this from now on.	
		OK Cancel	

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

Import Keys from File   Export Keys to File   Send Public Keys by Email   Compose Email to Selected Keys   Create Autocrypt Setup Message   Manage SmartCard   Reload Key Cache   Close   Ctrl+W   Exit	ile <u>E</u> dit <u>V</u>	<u>(</u> iew <u>K</u> eyserver <u>G</u> enerate				
Export Keys to File   Send Public Keys by Email   Compose Email to Selected Keys   Create Autocrypt Setup Message   Manage SmartCard   Reload Key Cache   Close   Ctrl+W   Exit	<u>I</u> mport	Keys from File	₽ Display All Keys	by Default		
Create Autocrypt Setup Message       Manage SmartCard       Reload Key Cache       Close     Ctrl+W       Exit	<u>Export</u>	<u>E</u> xport Keys to File Send Public Keys by Email Compose Email to Selected Keys	D 803C219B56CB	^ Type pub		E,
Manage SmartCardReload Key CacheCloseCtrl+WExit	Create	Autocrypt Setup Message	DB5A528CD41A1	pub/sec		
Reload Key Cache       Close     Ctrl+W       Exit	<u>M</u> anag	e SmartCard				
Close Ctrl+W Exit	<u>R</u> eload	Key Cache				
Exit	<u>C</u> lose	Ctrl+W				
	Exit					



#### 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.

🖳 Write: This is a	a test		$\times$
Eile Edit ⊻iew ☐ Send ↓ ✓ S	Insert Format Options Enigmail Tools Help pelling 👻 🕕 🙀 🎣 🐺 ave 👻		
From			~
∀ To	Valentin Besleaga <valentin.besleaga@camscape.ro></valentin.besleaga@camscape.ro>		
∀ To			
<u>S</u> ubject	: This is a test		
Paragraph 🗸	Variable Width ✓ 📕 🗛 · A' A' A A A 🗄 🗄 ½二   · 🗐 · 🔘 ·		
	"Valentin Besleaga <besleaga.valentin@gmail.com>"       X         4096-bit RSA key, ID DE8DBSA528CD41A1, created 2018-07-05.       Image: Comparison of the second secon</besleaga.valentin@gmail.com>		
Creating mail me	ssage		