

Installing and using PGP

The following paper describes how to install and use PGP.

This document is not static. Check for updates regularly.

History: V1.00 - *Initial release*

Overview

- Install GNUPG (GNU Privacy Guard)
- Install Thunderbird 1.5
- Create PGP Key
- Write an encrypted email



Install GNUPG

- 1. Download the GNUPG for Windows http://www.gnupg.org/download/index.html#auto-ref-1
- 2. Start the installer



3. Click next

🗑 GNU Privacy Guard Setup		Click on next
	Welcome to the GNU Privacy Guard Setup Wizard GnuPG is GNU's tool for secure communication and data storage. It can be used to encrypt data and to create digital signatures. It includes an advanced key management facility and is compliant with the proposed OpenPGP Internet standard as described in RFC2440.	
	Click Next to continue.	
	This is GnuPG version 1.4.5 built on 2006-08-01 11:22 UTC file version 1.4.5.21311	
	Next > Cancel	



4. Click next

🗑 GNU Privacy Guard Setup 🔤 💻	Click on next
License Agreement This software is licensed under the terms of the GNU General Public License (GPL) which guarantees your freedom to share and change Free Software.	VIIIO
Press Page Down to see the rest of the agreement.	
GNU GENERAL PUBLIC LICENSE Version 2, June 1991	
Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.	
Preamble	
The licenses for most software are designed to take away your	-
In short: You are allowed to run this software for any purpose. You may distribute it as long as you give the recipients the same rights you have received.	g
Nullsoft Install System v2.06	
< Back Next > Cance	

5. Click next

🗑 GNU Privacy Guard Setup 🖉 💶 🗙	Click next
Choose Components Choose which features of GNU Privacy Guard you want to install.	
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.	
Select components to install:	
Space required: 4.3MB	
Nullsoft Install System v2,06	



6. Click next

🗑 GNU Privacy Guard Setup		Click next
Install Options GnuPG Language Selection		
en - English		
Nullsoft Install System v2.06	1	
< Back Next >	Cancel	

7. Choose location

7. Choose location		
🌍 GNU Privacy Guard Setup	8_IX	Choose location
Choose Install Location Choose the folder in which to install GNU Privacy Guard.		
Setup will install GNU Privacy Guard in the following folder. To install in a different fo Browse and select another folder. Click Next to continue.	older, dick	
Destination Folder C:\Programme\GNU\GnuPG Browse	2	
Space required: 4.3MB		
Nullsoft Install System v2.06	Cancel	



8. Choose Startup Folder

🗑 GNU Privacy Guard Setup		Start Installation
Choose Start Menu Folder	NUMBER	process
Choose a Start Menu folder for the GNU Privacy Guard shortcuts.	U	
Select the Start Menu folder in which you would like to create the program's shorte	uts. You	
can also enter a name to create a new folder.		
GNU Privacy Guard		
7-Zip Accessories	-	
ACD Systems		
Acronis Autostart		
AviSynth 2.5		
Brenner Cain		
devolo		
Drucker DVD	-	
Do not create shortcuts		
Nullsoft Install System v2.06		
< Back Install	Cancel	

9. Continue

): Comme		
🕞 GNU Privacy Guard Setup	8_O×	Click next
Installation Complete		
Setup was completed successfully.		
	~	
Concluded		
Completed		
Show details		
Nullsoft Install System v2.06		
< Back Next >	Cancel	
S DOCK TRACE		



10. Finish installation



The installation of GNU Privacy Guard is now finished.



Install Thunderbird

11. Download the Mozilla Thunderbird for Windows http://www.mozilla.com/en-US/thunderbird/

^{12.} Start the installer





13. Accept License Agreement

Software License Agreement	a ×	Accept License
Software License Agreement Terms and conditions for using this software.	٩	Agreement
Please read the following license agreement. Use the scroll bar to view the rest of this agreement.		
FOR TRANSLATIONS OF THIS LICENSE INTO SELECTED LANGUAGES, PLEASE VISIT WWW.MOZILLA.ORG/LICENSING.	1	
MOZILLA THUNDERBIRD END-USER SOFTWARE LICENSE AGREEMENT Version 1.1		
A SOURCE CODE VERSION OF CERTAIN THUNDERBIRD BROWSER FUNCTIONALITY THAT YOU MAY USE, MODIFY AND DISTRIBUTE IS AVAILABLE TO YOU	•	
I Accept the terms of the License Agreement		
O I do NOT Accept the terms of the License Agreement		
< Zurück Weiter > Ab	brechen	

14. Choose Setup Type

Setup Type	8	×	Choose Setup Type
Setup Type Choose setup options.	Ś		
Choose the type of Setup you prefer, then click Next.			
 Standard 			
Thunderbird will be installed with the most common options.			
C Custom			
You may choose individual options to be installed. Recommended for experien users.	iced		
< Zurück Weiter >	Abbrechen		



15. Summary

Select Components	a ×	Summary
Summary Ready to start installing Mozilla Thunderbird.	6	
Setup will now install the following components:		
🎯 Mozilla Thunderbird, and:		
- Quality Feedback Agent		
to the following location:		
🗀 C:\Programme\Mozilla Thunderbird		
Click Next to continue.		
< Zurück Weiter >	Abbrechen	

16. Installation process

Installing	8	×	Installation process
Installing Installing Mozilla Thunderbird	6		
Currently installing Offline Support			
< Zurück Weiter > Ab	obrechen		



17. Finish installation and start Thunderbird

Install Complete		8	×	Finish installation
	Install Complete			and start Thunderbird
	Mozilla Thunderbird was successfully installed.			
	Launch Mozilla Thunderbird now.			
	Click Finish to complete Setup.			
	< Zurück Fertig stellen A	bbrecher		

18. Start Thunderbird and import Wizard

Import Wizard	Import Options, Account
Import Settings and Mail Folders From	Settings and other data if necessary.
Import Options, Account Settings, Addressbook and other data from:	
Outlook Express	
© Qutlook	
Don't import anything	
< Back Next > Cancel	



19. Start the installer

Account Wizard	a	X	Run the Account wizard
New Account Setup			(displayed automatically)
In order to receive messages, you first Newsgroup account. This Wizard will collect the information n Newsgroup account. If you do not know please contact your System Administrat	need to set up a Mail or ecessary to set up a Mail or the information requested, or or Internet Service Provider.		
Select the type of account you would lik	e to set up:		
< Ba	ck Next > Cancel		

20. Enter your identity

Account Wizard	,	8	×	Enter your Identity (name and email
Identity				address)
Each account has an you to others when	identity, which is the information that identifies they receive your messages.			
Enter the name you outgoing messages (would like to appear in the "From" field of your for example, "John Smith").			
Your Name:	PGP_Test Account			
Enter your email add email to you (for exa	ress. This is the address others will use to send ample, "user@example.net").			
Email Address:	pgptest@red-database-security.com			
	< Back Next > C	ancel		



21. Specify Server Information

Account Wizard	3 >	×1	Specify Server Information
Server Information			
Select the type of incoming server you are using.			
Enter the name of your incoming server (for example, "mail.example.net").			
Incoming Server: pop3.1und1.com			
Uncheck this checkbox to store mail for this account in its own directory. That will make this account appear as a top-level account. Otherwise, it will be part of the Local Folders Global Inbox account.			
✓ Use Global Inbox (store mail in Local Folders)			
Enter the name of your outgoing server (SMTP) (for example, "smtp.example.net").			
Outgoing Server: imap. 1und 1.com			
< Back Next > Can	el		

22. Choose User Names

Account Wizard	×	Choose User Names
User Names		
Enter the incoming user name given to you by your email provider (for example, "jsmith").		
Incoming User Name: pgptest		
Enter the outgoing user name given to you by your email provider (this is typically the same as your incoming user name).		
Outgoing User Name: pgptest		
< Back Next > Cance		



23. Choose Account Name

Account Wizard	8	×	Choose Account Name
Account Name			
Enter the name by which you would like to refer to this account (fo example, "Work Account", "Home Account" or "News Account").	r		
Account Name: pgptest@red-database-security.com			
		_	
< Back Next >	Cancel		

24. Finish Account Wizard

Account Wizard	<u>8</u>	×	Finish Account Wizard
Congratulations!			
Please verify that the informat Account Name: Email Address: Incoming User Name: Incoming Server Name: Incoming Server Type: Outgoing User Name (SMTP)	ion below is correct. pgptest@red-database-security.com pgptest@red-database-security.com pgptest pop3.lund1.com POP3 pgptest : imap.lund1.com		
Click Finish to save these setti	ngs and exit the Account Wizard.		



25. Choose Default Mail Application

Mozilla Thunderbird	8	×	Choose Default Mail Application
Do you want to use Mozilla Thunderbird as the default ma	il application	1?	

26. Thunderbird is started

💐 Inbox - Thunderbird		Thunderbird is
<u>File Edit View Go M</u> essage	[ools Help	
Get Mail Write Address Book	Reply Reply All Forward Delete Junk Print Stop	started
Folders	View: All	
E Coal Folders	Welcome to Mozilla Thunderbird! Mozilla Thunderbird is a powerful, open-source mail and news client. Features • Adaptive Junk Mail Controls • RSS Reader • Global Inbox Support • Saved Search Folders • Message Grouping • Privacy Protection More Information For frequently asked questions, tips and general help, visit Thunderbird Help. For product information, visit the Thunderbird Product Page.	



27. Save Enigmail Extension for Thunderbird on the harddisk

https://addons.mozilla.org/thunderbird/71/

Thunder	bird Add-ons	search: Go	Save the Enigmail extension to the
Home Extension	s Plugins Search Engines Themes		harddisk (e.g. C:\)
Enigmail	Enigmail » Overview	Rating: 3.97	
Overview	Enigmail 0.94.1, by Patrick Brunschwig,	A laine special functions (b) (in (in (in space logical (in space))))	
Previews & Screenshots	released on Aug 6, 2006 OpenPGP message encryption and	Note Note <td< td=""><td></td></td<>	
Comments	authentication.	Compared Temporal Temporal Temporal Compared to Temporal Tempora Tempora Tempor	
Add a Comment	Works with:	This is a signed and warryind meaning	
Version History	Thunderbird 1.5 - Linux, MacOSX,	9 Uver18 1961 - 8.95	
About the Author	Vindows	More Previews »	
Find Similar Add-ons	~		
Privacy and Security	Tinstall Now for Windows (288 KB)		
Other Thunderbird	Other Versions		
Add-ons	How to Install in Thunderbird:		
	 Right-Click the link above and choose "Save save the file to your hard disk. 	e Link As" to Download and	
	 In Mozilla Thunderbird, open the extension Menu/Extensions) 	manager (Tools	
	 Click the Install button, and locate/select t click "OK" 	he file you downloaded and	

28. Start the installer

Extensions	Choose the enigmail
	extension from the
Talkback 1.5.0.7 Submit a crash report to Mozilla.org.	location (e.g. C:\)
Install Uninstall Options Image: Section 2 and section 2 a	



29. Install Extension

Software Installation	8	×	Install Extension and restart Thunderbird.
A web site is requesting permission to install the item:	following		
enigmail-0.94.1-tb-windows	Unsigned		
from: file:///C:/enigmail-0.94.1-tb-v	windows.xpi		
Malicious software can damage your computer o your privacy. You should only install software from sor you trust.	or violate urces that		
Install (5)	Cancel		

30. Now we see the Menue OpenPGP

🍣 Inbox - Thunderbird							
E	ile	<u>E</u> dit	<u>V</u> iew	Go	Message	Ope <u>n</u> PGP	<u>T</u> ools
	5						
	1	•	E.			26P	
G	Get M	ail	Write	Addr	ress Book	Decrypt	

31. Open OpenPGP Key Management

				Open OpenPGP
<u>File Edit View K</u> eyserver <u>G</u> enerate				Key Management
Filter for user ID's or key ID's containing:	and choose			
Account / User ID	Key ID Type	Calcula Owner	Expiry 🛤	Generate New Pair from the menue.





32. Generate OpenPGP Key

Generate OpenPGP Key) ×	Choose your language
Account / User ID PGP_Test Account <pgptest@red-database-security.com> - pgptest@red-database-security.com> - pgptest@red-</pgptest@red-database-security.com>	ecu 🔻	
✓ Use generated key for the selected identity		
No passphrase		
Passphrase Passphrase (repeat)		
Comment		
Key expiry Advanced		
Key expires in 5 years 💌 🗖 Key does not expire		
Generate key Cancel		
Key Generation Console NOTE: Key generation may take up to several minutes to complete. Do not exit the application w generation is in progress. Actively browsing or performing disk-intensive operations during key generation w replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is comp	vhile key vill leted.	

33. Enter Passphrase for PGP key

Generate OpenPGP Key	X	Enter Passphrase
Account / User ID PGP_Test Account <pgptest@red-database-security.com> - pgptest@red-database-security.com> - pgptest@red-</pgptest@red-database-security.com>		
No passphrase Passphrase Passphrase (repeat) ********		
Comment Testkey		
Key expiry Advanced		
Key expires in 5 years 💌 🗖 Key does not expire		
Generate key Cancel		
Key Generation Console NOTE: Key generation may take up to several minutes to complete. Do not exit the application while generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is complete	e key ed.	





34. Advanced

Generate OpenPGP Key 🕘 🗴	Choose key size
Account / User ID PGP_Test Account <pgptest@red-database-security.com> - pgptest@red-database-secu</pgptest@red-database-security.com>	4096 in tab "Advanced"
Comment Testkey	
Key sze 4096 V Key type DSA & El Gamal V	
Generate key Cancel	
NOTE: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.	

35. Generate the key

OpenPGP Confirm	8	×	Generate
Generate public and private keys for 'PGP_Test Account (Testkey) <pgptest@red-database-security.com>'?</pgptest@red-database-security.com>			the key



36. Key will be generated

Generate OpenPGP Key	Key will be
Account / User ID PGP_Test Account <ppptest@red-database-security.com> - pgptest@red-database-secu •</ppptest@red-database-security.com>	generated
✓ Use generated key for the selected identity	
□ No passphrase	
Passphrase ****** Passphrase (repeat) *******	
Comment Testkey	
Key expiry Advanced	
Key size 4096 💌	
Key type DSA & El Gamal 💌	
Generate key Cancel	
Key Generation Console	
NOTE: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will	
replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.	

37. Key Generation completed

OpenPGP Confirm	OpenPGP Confirm 🔤 🔰
Key generation completed! Identity <pgptest@red-database-security.com> will be used for signing. certicate We highly recommend to create a revocation certificate for your key. This certificate can be used to invalidate your key, e.g. in case your secret key gets lost or compromised. Do you want to create such a revocation certificate now? certicate</pgptest@red-database-security.com>	Key generation completed! Identity <pgptest@red-database-security.com> will be used for signing. We highly recommend to create a revocation certificate for your key. This certificate can be used to invalidate your key, e.g. in case your secret key gets lost or compromised. Do you want to create such a revocation certificate now? Yes No</pgptest@red-database-security.com>



38. Create and Save Revocation Certificate

Create & Save R	levocation Certifi	icate			8	? ×	Create and
Speichem in:	Cols		- 6) 🔊 🖻 🛄-			Save Revocatio
Zuletzt verwendete D Desktop Eigene Dateien Arbeitsplatz	asm						n Certificate
Netzwerkumge	Dateiname:	d-database-security.com	(0x9B061701) i	rev.asc 💌	Speid	hem .	
Bung	Dateityp:	ASCII Armored Files (*.as	c)	•	Abbre	chen	

39. Enter OpenPGP passphrase

OpenPGP Prompt	×	Enter OpenPGP passphrase
Please type in your OpenPGP passphrase or your SmartCard P	PIN	

Remember for 5 idle minutes		
OK Cancel		

40. Revocation certificate created

OpenPGP Alert	Revocation
The revocation certificate has been successfully created. You can use it to invalidate your public key, e.g. in case you would lose your secret key.	certificate
Please transfer it to a medium which can be stored away safely such as a CD or Floppy Disk. If somebody gains access to this certificate they can use it to render your key unusable.	created



41. Key generated

🥞 Open	PGP Key Management					8.		The Key is
<u>File E</u> d	dit <u>V</u> iew <u>K</u> eyserver <u>G</u> enerate							now
Filter for	user ID's or key ID's containing:		<u>C</u> lear	r				generated
Accou	int / User ID	Key ID	Туре	Calcula	Owner	Expiry	<u> </u>	
PGF	'_lest Account (lestkey) <pgptest@re< td=""><td>98061/01</td><td>pub/sec</td><td>ultimate</td><td>ultimate</td><td>22.10.2011</td><td></td><td></td></pgptest@re<>	98061/01	pub/sec	ultimate	ultimate	22.10.2011		

42. Create an email

🐒 Compose: This is my first encrypted email with OpenPGP 🛛 🗐 💶 🗙	Create an email
<u>File Edit Vi</u> ew Insert Format Options OpenPGP Tools Help	
Send Contacts Spell Attach S/MIME Save	
From: PGP_Test Account <pgptest@red-database-security.com> - pgptest@red-database-security.com</pgptest@red-database-security.com>	
To: 💽 test@test.com	
Subject: This is my first encrypted email with OpenPGP	
This is a test	



43. Choose OpenPGP – Encrypt Message and click on send

OpenPGP Key Selection	a x	Choose
		Recipients for
test@test.com		Encryption and
Select Recipients for Encryption]	click OK.
Account / User ID Trust	Expiry Key ID 🖽	
PGP_Test Account (Testkey) <ppptest@red-database-security.com> ultimate</ppptest@red-database-security.com>	22.10.2011 9B061701	
Send mail unencrypted and not signed		
Do not display this dialog again if encryption is not possible		
Refresh Key List Download missing keys		

44. If you are using HTML email you are getting this warning

OpenPG	Alert 🗃	×	Skip
	HTML mail warning: This message may contain HTML, which could cause signing/encryption to fail. To avoid this in the future, you should press the SHIFT key when clicking on the Compose/Reply button to send signed mail. If you sign mail by default, you should uncheck the 'Compose Messages in HTML' preference box to permanently disable HTML mail for this mail account. This alert will repeat 1 more time.		



45. Send the encrypted email

🜠 Compose: This is my first encrypted email with OpenPGP 🛛 🗃 🗖 🔍	Choose your
File Edit View Insert Format Options OpenPGP Tools Help	language
	language
Send Contacts Spell Attach S/MILME Save	
From: PGP_Test Account <pgptest@red-database-security.co attagnments:<="" pgptest@red="" td="" ▼=""><td></td></pgptest@red-database-security.co>	
To: Est@test.com	
Subject: This is my first encrypted email with OpenPGP	
Body Text Variable Width	
BEGIN PGP MESSAGE	
Charset ISO-8859-1	
Version: GnuPG v1.4.5 (MingW32)	
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org	
hQQOA8iO4mQX1C8CEA/6A9Rq9H0rWx6/0bLd5+dR7xuYXRmVDo5JVPu1ZuIEjHdd	
4vPpuKNCghwgKRVFBvSb4kSO6u8SIzY+59X2UVHTikV9eC+OrZz8IYJuJ29zr17u	
zJAUXHFhbsUwi2D5GOUMeJ48yCdVEQh4H8lsMtpdX/lwYWKADi6SD/xdCPUCYqg9	
x11xA0/NTbIAtFcqLEyivtYs1BssBth6GblU0pVeYvPc1PfRdB/E3TWzEd6LD0y5	
yajcndAqeo+vv4LBEGQK9N1nc7h04TpyKqEZzYYj/X8SSdsiqYBB8J4LydplmjIj	
RkdK1HY9WAaqyFsRnfZFMJeaWMP7LKMjXLobLTZJfKQaTDVdtxJg7iTPBzAPMzU6	
s62hrwW9z3p9XHAOa4HZ7L9EUx58C8g8o5FRcGBnk6OejjXOlkkmWGYXy+/c7w75	
CnMmKcLhYJmvAdRfWE5BCBWJLQlu5bhwgBDryZZ223XMoghc+DmbBqOUf4JkwLr3	
HWcJSShSjWdumoGWSJGU1pVVfbBErTRmuVJJ78AfLLXUxyjmVkp9k0+is4b41wo7	
0TTQQfMQeXI4u9HNNT8usz1a9qiT28m4nfp0ZR8qebqNx8g2eLI/cfMJN8+s6u65	
FOjj92xN2WdJk+Ou2DdWeofMQc+B+HgDdAJyrmkJDlR9CoVmlGpS01YqbrRArL0Q	
AKY2F+j7x8PkQF44xuUGu/iCBQHNgPD0A8gYuB8ENNzHq2GP9kK1uESK4AoXvrFq	
btItubbtZJT8InoBOPAvTQpruXsnUGK1+KVu4yXShYj9cXICT9tuOy3XhkuX0e3Z	
ek8PFck5JDDJk38K4I4T27MVFw8E/jB+zvCs26q5zY42KZgyZfaFEGKKGXijL/zz	
2AjM0izRw30XkAgvLSkIaF8QLLI9F928I/UnD9TkVfNYoKcy8+7dOL+wMeze6PBA	
aSE81bmhvKY2u2BGX5cZezIXbfKYM2GHleTej4xDr3Pn0fs/3cVl993fXBmko7Cm	
t3MHRqoHIJcsJwCZJRx4vfn5ycIIIP112bQ4CuMY9KKsLhkwYcXHbnkOZR7CPRzM	
5ME9FUnAZXicUqdMvTSGquEOtr0qioKhO7aamAr6L569ZGLBrzPbZbtv6/FdB4zp	
lcNxul8v2DRsHosi3Eg/F4ievmS++M/Yaj7MxZTqmv3SfLNbKhBVilFoBTlfFUEb	
F5OzeHWI83uyBNZotZq1fT5k8M0Zjb2NDfCsAnpJtWoG9TF9rgoq9VNy1AHFGv8z	

That's it ...



Related Links:

Download GNUPG: <u>http://www.gnupg.org/download/index.html#auto-ref-1</u>

Download Mozilla Thunderbird: http://www.mozilla.com/en-US/thunderbird/

Download Enigmail Extension for Thunderbird: https://addons.mozilla.org/thunderbird/71/

About Red-Database Security GmbH:

Red-Database-Security GmbH is a specialist in Oracle Security. We are offerings Oracle security trainings, database and application server audits, penetration tests, oracle (security) architecture reviews and software security solutions against Oracle rootkits.

Contact:

If you have questions or comments you could contact us via

info at red-database-security.com