

KU



PGP Encryption for Windows

Ankit Agarwal

Department of Electrical Engineering & Computer Science GPG4Win software presentation

ankit@ku.edu



PGP Encryption for Windows Outline

- Introduction to GPG
- GPG4Win software
- Installation and Configuration of GPG4Win
- Using GPG4Win
- References



PGP Encryption for Windows Outline

- Introduction to GPG
- GPG4Win software
- Installation and Configuration of GPG4Win
- Using GPG4Win
- References



PGP Encryption for Windows Introduction

- What is GPG?
 - GPG stands for GNU Privacy Guard
 - Free implementation of the OpenPGP standard as defined by RFC4880
 - Allows you to encrypt and sign data and communication
- Website:

http://www.gnupg.org/



PGP Encryption for Windows Outline

- Introduction to GPG
- GPG4Win software
- Installation and Configuration of GPG4Win
- Using GPG4Win
- References



PGP Encryption for Windows GPG4Win software

- Software implementation of GPG for Windows
- Both cryptography standards are supported, OpenPGP and S/MIME
- Website:

http://www.gpg4win.org/



PGP Encryption for Windows GPG4Win software

GnuPG:	The core; this is the actual encryption tool
WinPT:	A key manager and helper for various encryption matters
GPA:	Another key manager, tasts are simply different
GPGol:	A plugin for Microsoft Outlook 2003 (email encryption)
GPGee:	A plugin for Microsoft Explorer (file encryption)
Claws Mail:	A complete email program including the plugin for GnuPG
Documentation:	
Gpg4win for Novices:	A handbook specifically for newbies
Gpg4win für Durchblicker:	A (German!) handbook about some background, for beginners
	Erom [2]

From [2]



PGP Encryption for Windows Outline

- Introduction to GPG
- GPG4Win software
- Installation and Configuration of GPG4Win
- Using GPG4Win
- References



License Agreement	· · · · · · · · · · · · · · · · · · ·
This software is licensed under the terms of the GNU General Public License (which guarantees your freedom to share and change Free Software.	(GPL)
Press Page Down to see the rest of the agreement.	
GNU GENERAL PUBLIC LICENSE Version 2, June 1991	1
Version 2, June 1991	
Copyright (C) 1989, 1991 Free Software Foundation, Inc.	
51 Franklin Street, 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 dist	tribute it as long
as you give the recipients the same rights you have received.	
Vullsoft Install System v2.19-3	

September 16, 2008



😚 GnuPG For Windows Set	ир	
Choose Components Choose which features of Gnu	PG For Windows you want to insta	all.
Check the components you wa install. Click Next to continue.	nt to install and uncheck the comp	oonents you don't want to
Select components to install:	GnuPG GnuPG2 GPGol GPA WinPT GPGee	Description Position your mouse over a component to see its description.
Space required: 19,9MB	Claws-Mail Claws-Mail Novice Manual	
Nullsoft Install System v2.19-3 —		
	< Back	Next > Cancel

September 16, 2008



Choose Install Location Choose the folder in which to insta	all GnuPG For Windows.	(
Setup will install GnuPG For Windo click Browse and select another fo	ws in the following folder. To install in a d Ider. Click Next to continue.	ifferent folder,
Destination Folder]
Destination Folder C:\Program Files\GNU\GnuPG		Browse
		Browse
C:\Program Files\GNU\GnuPG		Browse



🗑 GnuPG For Windows Setup	
Install Options Start links	
Please select where Gpg4win shall install links:	
Start Menu	
Desktop	
Quick Launch Bar	
(Only programs will be linked into the quick launch bar.)	
Nullsoft Install System v2,19-3	
< Back Next >	Cancel



noose Start Menu Folder		1
hoose a Start Menu folder for the (GnuPG For Windows shortcuts.	(
	n you would like to create the program	n's shortcuts. You
an also enter a name to create a ne GnuPG For Windows	ew rolder.	
Accessories		
Administrative Tools Games		
Aozilla Firefox Sophos		
Startup		



🗑 GnuPG For Windows Setup		
Installing Please wait while GnuPG For Windows is b	being installed.	
Extract: gpgol.dll 100%		
Show details		
Nullsoft Install System v2,19-3		
	< Back Next :	> Cancel



😽 GnuPG For Windows Set	tup
	Completing the GnuPG For Windows Setup Wizard GnuPG For Windows has been installed on your computer.
	Click Finish to close this wizard,
	Show the README file
	Click here for the project's homepage
	< Back Finish Cancel

September 16, 2008





September 16, 2008







	-	and the second s		And a second
Kev		огат	inn w	izard
		CI ULL		12 01 0

X

Name and E-Mail Assignment

Every key pair must have a name associated with it. The name and email address let your correspondents know that your public key they are using belongs to us.

Real name:	Test Email

By associating an email address with your key pair, you will enable WinPT to assist your correspondents in selecting the correct public key when communicating with you.

Email address: TestEmail@abc.com

Prefer RSA keys

12 .

GPG4Win

OK

Cancel



Key Generation	
Repeat Passphrase	
*******	🔽 Hide Typing
	OK Cancel



By associating an ema WinPT to assist your c key when communicat		ust have a name associated wi your correspondents know that	
By associating an ema WinPT to assist your c key when communicat OK	Real name: Test B	GnuPG Status 🛛 🔯)
imail address: TestEmail@abc.com	By associating an ema WinPT to assist your c key when communicat		will enable
	Email address: TestE	mail@abc.com	



estination for	Public Keyring			?
Save in:	C KeyRingBack	<u>•</u>	• 🗈 💣 📰 •	
My Recent Documents				
B				
Desktop				
My Documents				
My Computer				

September 16, 2008



Key Generation	Wizard			×	
Destination for	Secret Keyrin	8			?
Save in:	🚞 KeyRingBad	sk	•	+ 🗈 💣 📰 -	
My Recent Documents Desktop	pubring_bak.	gpg			
My Documents					
	File name:	lsecrina bak		.	Save

September 16, 2008



PGP Encryption for Windows Outline

- Introduction to GPG
- GPG4Win software
- Installation and Configuration of GPG4Win
- Using GPG4Win
- References









Septem

Clipboard Ed	litor	
File Edit GPG	5	
This i	Encrypt essage	
Сору	-	
16, 2008	GPG4Win	





is is	er ID	Key ID	Size	Cipher	Validity
	₩ Test Email <testemail@abc.com></testemail@abc.com>	0xC85BE559	2048	RSA	Ultimate
Find	key: Find			0K	Cancel



Clipboard Editor	
File Edit GPG	
BEGIN PGP MESSAGE Version: GnuPG v1.4.7 (MingW32) - WinPT 1.2.0 hQEMAxUmkI/IW+VZAQf9GtVU6rLHGaPu2ECPViRhOFKp3NiDfrphMk362VPGY1mB Rbe5qiHACVvdFtxzLTKeoO5G7pMW8afUy67O0Q2aJ8PGbDu0EEtVCq9Jh9m8tMHZ j/AyI1zTqtKyhVWIEcCCwj11zpdVApWqLCsbU/VfjjPMxCz7aGd+Ought7S+Qz2o gW/STXK4ASELcsWQe1nnTQIUziDq9K4FIj96yKppDJxh50VnN4FpsT49CRM2rDnA ed1mAY7vVqyX/wqJGjQ08a26xmFgxShbdnf1VSdix/v6kDW+oLYGxQQ31hj7040w vWxdj+PywFcuNnJrDRZ994s1B16BXN8WNN8WnphsxtJQAcrm5J19p0QCutbJE/ef iPO9NeyeIN4mzmjAzbiZ4p88zBgKpV/vaiAB9oWGoG9SmIt9Lo8Uvb9Fi9oV109w NgqL80BvB/OB142SJAR/jp0= =CfXf END PGP MESSAGE	
Сору	



Clipboard Editor	
File Edit GPG	
Versio Decrypt 1.4.7 (MingW32) - WinPT 1.2.0	
hQEMAxUmkI/IW+VZAQf9GtVU6rLHGaPu2ECPViRhOFKp3NiDfrphMk362VPGY1mB Rbe5qiHACVvdFtxzLTKeoO5G7pMW8afUy6700Q2aJ8PGbDu0EEtVCq9Jh9m8tMHZ j/AyI1zTqtKyhVWIEcCCwj11zpdVApWqLCsbU/VfjjPMxCz7aGd+Ought7S+Qz2o gW/5TXK4A5ELcsWQe1nnTQIUziDq9K4FIj96yKppDJxh50VnN4FpsT49CRM2rDnA ed1mAY7vVqyX/wqJGjQ08a26xmFgxShbdnf1VSdix/v6kDW+oLYGxQQ31hj7040w vWxdj+PywFcuNnJrDRZ994s1B16BXN8WNN8WnphsxtJQAcrm5J19pOQCutbJE/ef iPO9NeyeIN4mzmjAzbiZ4p88zBgKpV/vaiAB9oWGoG9SmIt9Lo8Uvb9Fi9oV109w NgqL80BvB/OB142SJAR/jp0= =CfXf END PGP MESSAGE	
Сору	



Clipboard Editor		×
File Edit GPG		
BEGIN PGP MESSAGE Version: GnuPG v1.4.7 hQEMAxUmkI/IW+VZAQf9G Rbe5qiHACVvdFtxzLTKeo j/AyI1zTqtKyhVWIEcCCw gW/STXK4A5ELcsWQe1nnT ed1mAY7vVqyX/wqJGj008 vWxdj+PywFcuNnJrDRZ99 iPO9NeyeIN4mzmjAzbiZ4 NgqL80BvB/OB142SJAR/jj =CfXf END PGP MESSAGE-	Occryption Image: Constraint of the second seco	
Copy		

September 16, 2008



File Edit GPG This is a test message <u>Copy</u>	Clipboard Editor		
	File Edit GPG		
Сору	This is a test	essage	
Сору			
Сору			
<u>С</u> ору			
Сору			
	<u>С</u> ору		
GPG4Win			



PGP Encryption for Windows Outline

- Introduction to GPG
- GPG4Win software
- Installation and Configuration of GPG4Win
- Using GPG4Win
- References



PGP Encryption for Windows References

- 1. http://www.gnupg.org
- 2. http://www.gpg4win.org