UNCLASSIFIED

VARIABLECONSTANT PGP Security Instructions for Windows Date: 5/27/2018 Version 1.1

PGP Installation/Configuration Steps:

 PGP 4 Windows Download Link: <u>https://www.gpg4win.org/get-gpg4win.html</u>
 Selecting \$0 will allow one to download it, otherwise you can provide a donation.

,	Home » Download Download Gr You can also use this installer	994Win 3.1.1 (2018-05-03) to update an older version. Keys and configration will be kept.
	Please donate for Gp Pay what you want! – Thar	g <mark>4win to support maintenance and development!</mark> ik you!
	Donate with PayPal Bitcoin Bank transfer	PayPal S0 S10 S15 \$25 \$ USD EUR onetime monthly Add me to the list of sponsors (from 20,- EUR/USD up) I am using Gpg4win because
		Donate & Download

2. Install the Downloaded App (Select GnuPG, Kleopatra, GpgOL, GpgEx)

Gpg4win Setup		
Gpg4win	Choose Components Choose which features of G	Gpg4win you want to install.
Check the components you install. Click Next to contin	u want to install and uncheck th ue.	ne components you don't want to
Select components to insta	all: GnuPG Kleopatra GPA GpgOL GpgEX	Description Position your mouse over a component to see its description,
Space required: 98.2MB		
Gpg4win-3,1,1		
	< Bac	ck Next > Cancel

3. Once Installed, Open Kleopatra



4. Click Settings -> Configure Kleopatra

e View Certificates Tools	Settings Window Help	
V. 10	Perform Self-Test	0
n/Encrypt Decrypt/Verify	Show Toolbar	Notepad
Search <alt+q></alt+q>	🚓 Configure Shortcuts	All Certificates
Name	🗉 Configure Toolbars	User-IDs
John Martellaro	📧 Configure Kleopatra Ctrl+Shift+,	certified 5/1

5. Click Crypto Operations

Check the box for Create OpenPGP Encrpyted files with ".pgp" file extensions instead of ".gpg" Click Ok

Directory Services	- EMail Operations
	Don't confirm signing certificate if there is only one valid certificate for the identity
Appearance	Don't confirm encryption certificates if there is exactly one valid certificate for each recipient
Δ	File Operations
	Create OpenPGP encrypted files with ".pgp" file extensions instead of ".gpg"
Crypto Operations	Automatically start operation based on input detection for decrypt/verify.
S	Create signed or encrypted files as text files.
S/MIME Validation	Create temporary decrypted files in the folder of the encrypted file.
Ω	Checksum program to use when creating checksum files: sha1sum
GnuPG System	Archive command to use when archiving files: TAR (PGP®-compatible)
	General Operations
	Activate gnuPG Prohie: Apply

6. Click File -> New Key Pair

K	eopatra	ala Cattinana	Madau	Lista	1000		-	
er:	New Key Pair	Ctrl+N	port	Certify	Q Lookup on Server	() Notepad		
	Lookup on Server	Ctrl+Snift+1 Ctrl+I						
		01.5					All Certificates	•
	Export	Ctri+E			E-Mail		User-IDs	F (4
=> ⊟	Print Secret Key			john@var	iableconstant.com		certified	5/1
	Publish on Server	Ctrl+Shift+E	L					
w	Decn/nt/Verify							
	Sign/Encrypt							
	Sign/Encrypt Folder		L					
	Create Checksum Files Verify Checksum Files							
	Close	Ctrl+W	I					
-	Quit	Ctrl+Q						
			_					
-								+

7. Select Create a personal OpenPGP key pair

UNCLASSIFIED



8. Fill in the Name Field, and Email Field your information, and Click Next

7

🕤 Kleopatra										
File View Cer	tificates	Tools	Settings	Window	Help					
Sign/Encrypt	777						0		8 x	Ŋ
Search <al< td=""><td>Key Pa</td><td>air Creati</td><td>ion Wizaro</td><td>ł</td><td></td><td></td><td></td><td></td><td>-</td><td>-</td></al<>	Key Pa	air Creati	ion Wizaro	ł					-	-
John M	Enter	Details								User-ID:
John III	Please e the Adva	nter your anced Set	personal o ttings butto	details belov on.	w. If you w	ant more	control o	ver the param	eters, <mark>click o</mark> n	lines
	Name:	First Nam	e Last Nan	ne					(optional)	
	EMail:	email@ad	ldress.com						(optional)	
			Fir	st Name Las	st Name <	email@ad	dress.com	> Advanc	ed Settings	
								Next	Cancel	

9. Click Create

incrypt	8 <mark>×</mark>
rch <al< td=""><td>G Key Pair Creation Wizard</td></al<>	G Key Pair Creation Wizard
John M	Review Parameters
John W	Please review the parameters before proceeding.
	Name: First Name Last Name Email Address: email@address.com
	Show all details

10. Create a Secure Password, Click Ok

Make it different than anything you have ever used before. You will use this frequently. A good way to make new passwords is to make a sentence.

(e.g.) I like to play tennis with my friends at 2PM on Sundays - Iltptwmfa2PMoS

7) Kleopatra File View Ce	rtificates Tools S	ettings Window Help	
Search<	Key Pair Creat Creating Key The process of c several minutes.	pinentry-qt Please enter the passphrase to protect your new key Passphrase: Repeat: Quality: OK Cancel	nay require
		Next	Cancel

11. Just Click Finish (**Do NOT** Upload Public Key To Directory Service)

/ Pair Successfully Created	
r new key pair was created successfully.	Please find details on the result and some
gested next steps below.	
esult	
(ey pair created successfully.	
Ingerprint: C8077B15F3B260CCB2DB1EC	JEF42BDF423836E5A8
ext Steps	
Make a Backu	p Of Your Key Pair
Send Publ	ic Key By EMail

12. Select the new entry, and then click File->Export

ile	View Certificates To	ools Settings	Window Help	
	New Key Pair	Ctrl+N		
Q	Lookup on Server	Ctrl+Shift+I	port Certify Lookup on Server Notepad	
	Import	Ctrl+I	All Certificates	•
	Export	Ctrl+E	E-Mail	User-ID
	Export Secret Keys		john@variableconstant.com	certified
Ģ	Print Secret Key			
	Publish on Server	Ctrl+Shift+E		
<u>ă</u>	Decrypt/Verify			
	Sign/Encrypt			
	Sign/Encrypt Folder			
	Create Checksum Files		_	
	Verify Checksum Files			
	Close	Ctrl+W		
-	Quit	Ctrl+Q		

UNCLASSIFIED

13. Save the public key. This is what you will share with others. My folder structure is PGP KEYS->Public Keys -> email associated with key (e.g. john@variableconstant.com) -> Public Key.

Kleopatra				
Export Certificates				×
) 🖓 🖉 🚺 « Pl	JBLIC K	EYS > john@variableconstant.com	- + Search john@	variableconstan 🔎
Organize 🔻 Ne	ew folde	er		E • 🔞
Favorites	-	Name	Date modified	Туре
Desktop Downloads OneDrive Recent Places Oreative Clou Libraries Documents	; d Fi	9FEE4AE981FFE24A461C2E9FD74DF7159D	. 5/27/2018 11:36 AM	OpenPGP Binary F
Music				
Videos	-	•		•
File name:	9FEE4	AE981FFE24A461C2E9FD74DF7159DBB37FE.pgp		.
Save as type:	Open	PGP Certificates (*.asc *.gpg *.pgp)	Sur	▼

Import PGP Keys

- Option 1: If the application is installed, you can either double click the public key someone shared, and Kleopatra will automatically add it.
- Option 2: Click Import from the Kleopatra Menu

	AT Q	
Sign/Encrypt Decrypt/Verify Import Export	Certify Lookup on Server Notepad	
Search <alt+q></alt+q>	All Cer	tificates
All Certificates Imported Certificates		
Name	E-Mail	User-ID
John Martellaro	john@variableconstant.com	certified

Encryption Example:

• From Kleopatra -> Click Notepad

🗊 Kleopatra	the Sector		100.000	
File View Certificates	Tools Settings Windo	w Help		
			Ø	
Sign/Encrypt Decrypt/V	erify Import Export	Certify Lookup on	Server Notepad	
Sign / Encrypt Notep	ad 🔯 Decrypt / Verify Notep	ad		
This is a secret	test message.			

- Click the Notepad Tab, and write the text you want encrypted
- Click the Recipients Tab and Fill Out the Information
 - Sign as: Check and put in your signing key
 - Encrypt for me: Check and put in your signing key
 - Encrypt for others: Put in all the emails of imported keys you want to share with
 - Do NOT Encrypt with Password (It's counter intuitive, it removes the need for PGP Keys, and is a way if you want to share a file with PGP key or to enter a password)

Kleopatra					
ile View Certificates	Tools Settings W	indow Help			
ign/Encrypt Decrypt/Verif	y Import Expo	Ē} Ē₽ ort Certify Lo	Q okup on Server	Notepad	
Sign / Encrypt Notepad	🕅 Decrypt / Verify N	otepad			
Prove authenticity (sign)					
Encrypt					
Encrypt for me:	📀 John Martellaro <j< td=""><td>ohn@variableconstant</td><td>.com> (certified, o</td><td>reated: 5/17/2018)</td><td>-</td></j<>	ohn@variableconstant	.com> (certified, o	reated: 5/17/2018)	-
Encrypt for others:	? Please enter a na	me or email address			
Encrypt with passwor	'd. Anyone you share th	e password with can r	ead the data.		

.	
ncrypt Decrypt/Verify.	Import Export Certify Lookup on Server Notepad
Sign / Encrypt Notepad	🕅 Decrypt / Verify Notepad
/Encrypt	🔓 pinentry-qt
Notepad 2+ Recipi Prove authenticity (sign) - Image: Comparison of the second	Please enter the passphrase to unlock the OpenPGP secret key: "John Martellaro "John Martellaro 2048-bit RSA key, ID D74DF71590BB37FE, created 2018-05-17.
Encrypt	Passphrase:
Encrypt for me:	OK Cancel
🛛 Encrypt for others: 🚶	
	? Please enter a name or email address

• Click Sign / Encrypt Notepad -> Enter the password with the key account you created

• Click Notepad Tab Again – Your Message has been Encrypted. Copy all of the text, and it can be shared via email.

👩 Kleopatra	
File View Certificates Tools Settings Window Help	
Image: Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server	
Sign / Encrypt Notepad X Decrypt / Verify Notepad Severt	
<pre>https://www.setup.com/ https://www.setup.com/ https://www.setup.com/ files/setup.com/ files/setup.com/ files/setup.com/ getup.c</pre>	

UNCLASSIFIED

Decryption Example:

• Copy a PGP Message into the Notepad Window

eopatra	x
View Certificates Tools Settings Window Help	
記 認 画 画 画 の Notepad	
Sign / Encrypt Notepad) 🔯 Decrypt / Verify Notepad) 🕤 Revert	
√ Notepad 2+ Recipients	
BEGIN PGP MESSAGE	
DEMA9x+HDYoOrKLAQf/RwjDpgXzSsgpq0TMomGCLEihRKkdVT4/0Jwd9A3RDR9P 10Y2914cPwcSEKciE/4d8tNgnvLezVm9s9NEcSknywtP/Lc/Ysmyoh0ppYftfFi	
JxB8kroqdkWMjnl6XaeC0+oCmPqst42s0yjQtFJzRGUzpE5AJoc3b6EYnbU77r	
/otKhuR6NxRByd+D7bL+AbwVlGZqH3DuOri11F72D+FND+XEu91epB53X1tR5Ay gnnTgi6g8gR3e67P7iESTMowKOTR3WsKluWpv≥o6fvrf0gmd40KhiNVwL5wPnaX	
Nnmsj3Cw4OwyZ1PkrgTvg2g3f0vZIDM/FCLkpN7+9LA4gFZHw5Fle8Jvh1fMI2d	
nuobTcVn5PjLfS061iKrytYsH463eOdkYhTOPfhsKaCLymET4ts66WRdxrp406J MhCUZuCoDmPK22x4as2iWeDiDCau3ar0/aDuShoasYsEaHlutYaoSMaJDuHfDNN	
ZtgjvvPRCvsP2iRsUNur5w1Cxn4FvSKsW1mOlicj5qC6bd99Q5qbTUCPi1W7dMw	
OVbU8m3HsPKxJLKo4z+TWc07fqkqSoEmxY0/TVWJJFe3IUnTK7aJqVnHDMwOVKj	
buYMARSXLRDVC19DE83PVnCa5ZfinHqnLpKpE70t19fjh+1mJ8pMAYpqZ2byyO2 Dov/c3XS2cCYqWiyxWsUatYMacCrSJmSmcH88qAW/S2Aa4f3vCWaR2kto9LxbUt	
dV/csr18PRk60UJn1Mo2GnLCQIzK4w5IKYhetmvg3v8Qufi/isxb028j2/+Qf1J	
aWCBX1cqszG0TMsvWsTqdnNwBo1Y5h9d2qvfhbmk3wCr0N+vAUOuAoPbiUgcaMi	
BMQ/OapldilPMeiTaDfzliH+cM=	
END PGP MESSAGE	

• Click Decrypt / Verify Notepad – If successful, it will decrypt the message

👩 Kleopatra	
File View Certificates Tools Settings Window Help	
المحمد الحجار Notepad Notepad Notepad Notepad	
Sign / Encrypt Notepad 🔯 Decrypt / Verify Notepad 5 Revert	
Notepad → Notepad: Valid signature by john@variableconstant.com Signature created on Sunday, May 27, 2018 12:16:12 PM With certificate: <u>9FEE 4AE9 8JFF E24A 461C 2E9F D74D F715 9D88 37FE</u> The signature is valid and the certificate's validity is ultimately trusted.	Close
This is a secret test message.	

Encryption / Decryption of Files

- Open a File Folder, and select the file you want to encrypt
- Right Click the file -> More GpgEX options -> Sign and encrypt

🗢 🗣 🍌 🕨 PGP Example			✓ 4 Search PGP Example	ole	P
Drganize ▼ ① Open ▼ ★ Favorites Nar ■ Desktop □ ↓ Downloads ▲ OneDrive	Share with Print	1	Open Print Edit Convert to Adobe PDF Combine files in Acrobat		• 🗋 🕑
Recent Places Creative Cloud Files			Edit with Notepad++ Sign and encrypt		
 □ Libraries □ Documents □ Music □ Pictures □ Videos □ Computer △ OS (C:) ① Network 			More GpgEX options Open with Share with Norton Security Add to archive Add to "Encryption Example.rar" Compress and email Compress and email Compress to "Encryption Example.rar" and email Restore previous versions Send to	• • •	Decrypt Verify Decrypt and verify Encrypt Sign Sign and encrypt Import keys Create checksums Verify checksums Help on GpgEX About GpgEX
Encryption Example Text Document	ie.txt Date modified: 5/27/201 Size: 0 bytes		Copy Create shortcut Delete		

• Enter Signing / Encryption Details

👩 Sign/Encrypt Files - I	Geopatra	? X
Sign / Encrypt Prove authenticity (sign) Sign as:	Files	l create ▼
Encrypt		
Encrypt for me:	🕗 John Martellaro <john@variableconstant.com> (certified</john@variableconstant.com>	l, create ▼
Encrypt for others:	? Please enter a name or email address	
Encrypt with passwor	d. Anyone you share the password with can read the data.	
Encrypt / Sign each f	le separately.	
: C:/Users/admi	n/Desktop/PGP Example/Encryption Example.txt.pgp	
	Sign / Encrypt	Cancel

• Encrypted File Can Now Be Shared (Will Have a PGP, or GPG extension depending on configuration)

🔾 🔍 🔻 📕 🕨 PGP Example		•	✓ Search PGP Exan			
Organize 👻 👩 Oper	r ▼ Share with ▼ New folder				•	. 0
🔆 Favorites	Name	Date modified	Туре	Size		
🧮 Desktop	Encryption Example.txt	5/27/2018 11:56 AM	Text Document		0 KB	
🐌 Downloads	Encryption Example.txt.pgp	5/27/2018 12:22 PM	OpenPGP Binary F		1 KB	
🝊 OneDrive						
📃 Recent Places						
Oreative Cloud Files						
🧊 Libraries						
Documents						
🛛 🎝 Music						

• For Decryption, follow the same steps, but select decrypt It will convert the pgp file back to its txt file.