# What is GPG?

See description here

## GPG for Windows users

There are several applications under the Windows operating system which allow you to generate a gpg key pair. Among the best known is Gnu4win with its module called [Kleopatra]. Gpg4win is a free distribution encryption software which allows the encryption of files and the sending of documents through email using public key cryptography for data encryption and digital signatures.



Supports cryptography OpenPGP and S/MIME (X.509) standards.

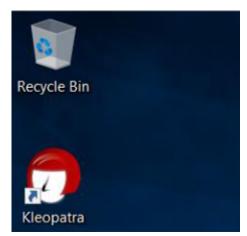
It consists of several modules, including:

- GnuPG : the basic encryption tool
- Kleopatra : certificate manager for OpenPGP y X.509
- GPA : an alternative certificate manager (GNU) for OpenPGP and X.509

#### GPG4win installation

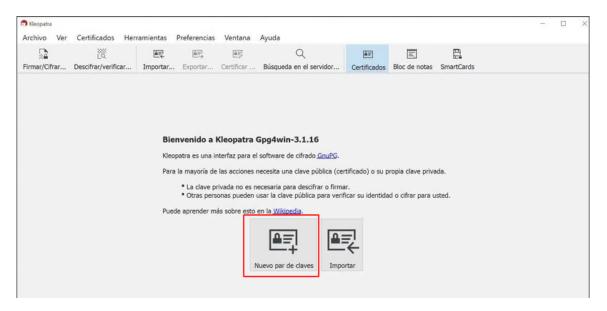
On the project website download the latest version of the software. Open the installer and authorize the changes if necessary. Follow the steps indicated with the Next button.

🔒 Gpg4win Setup	- 🗆 X
Gpg4win	Welcome to the installation of Gpg4win
GnuPG for Windows	Gpg4win is an installer package for Windows for EMail and file encryption using the core component GnuPG for Windows. Both relevant cryptography standards are supported, OpenPGP and S/MIME. Gpg4win and the software included with Gpg4win is Free Software.
	Click Next to continue.
	This is Gpg4win version 3.1.3 Release date 2018-08-31
	Next > Cancel
🔒 Gpg4win Setup 🛛 🖑	– 🗆 X
	boose Components hoose which features of Gpg4win you want to install.
Check the components you wa install. Click Next to continue.	nt to install and uncheck the components you don't want to
Select components to install:	GnuPG Position   Kleopatra Position your mouse over a component to see its description.   GPA See its description.   GpgOL GpgEX   Browser integration Image: Component to see its description.
Space required: 98.2MB	
Gpg4win-3.1.3	< Back Next > Cancel



#### Generate a key pair (public and private)

Once Gpg4win is installed we are going to use the *Kleopatra* module to generate a new gpg key pair. To do this, from the files tab we select *New Certificate* which will open the certificate generation wizard.



Click on Create a personal OpenGPG key pair

Asistente de creación del par de claves

#### Elegir formato

Por favor, elija qué tipo quiere crear.

Los p	ar un par de claves personales OpenPGP pares de claves OpenPGP están certificados por la confirmación de pública.	e la huella d	igital de la
Los p	ar un par de claves personales X.509 y una peticio pares de claves X.509 se certifican por una autoridad de certificaci rada necesita enviarse a la CA para finalizar la creación.		
		Next	Cancel
ter the re	equired data		
			? ×
Introd Por favor	e de creación del par de claves UZCA detalles , introduzca sus detalles personales debajo. Si desea más control sobre l onfiguración avanzada».	los parámetro	
Introde Por favor botón «C	uzca detalles , introduzca sus detalles personales debajo. Si desea más control sobre l	los parámetro	
Introde Por favor botón «C	uzca detalles , introduzca sus detalles personales debajo. Si desea más control sobre l onfiguración avanzada».	los parámetro	s, pulse el
Introd Por favor botón «C Nombre:	uzca detalles , introduzca sus detalles personales debajo. Si desea más control sobre l onfiguración avanzada».	los parámetro	s, pulse el
Introde Por favor botón «C Nombre:	uzca detalles , introduzca sus detalles personales debajo. Si desea más control sobre l onfiguración avanzada». Julián G.	los parámetro	s, pulse el
Introd Por favor botón «C Nombre:	uzca detalles , introduzca sus detalles personales debajo. Si desea más control sobre l onfiguración avanzada». Julián G. Proteger la clave generada con una frase de contraseña.		s, pulse el

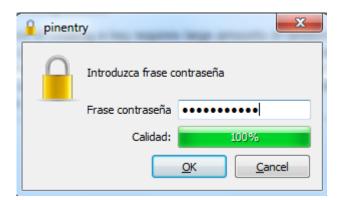
In the *Advanced Settings* tab, indicate a 4096 bits key length and an expiration date no more than 2 years.

👩 Advanced Settir	ngs						?	$\times$
Technical Details								
Key Material								- ا
	4,0	096 bit	s	1	•			
▼ +RSA	4,0	096 bit	35		•			
C <u>D</u> SA	2,0	048 bit	s (defa	ult)	~			
F + Elgame	al 2,0	048 bit	s (defa	ult)	Ψ.			
Certificate Usage								_
Signing				Certific	Ting			
l≪ <u>signing</u>			14	Gerund	auon			
Encryption				Authen	ticatio			
I≪ Encrypuon				Source	100300			
	2017-	12-31			locauo		€3 -	
	2017-		Decen	_	_	_	- B	
				nber	201	_		
			Decen Wed	nber	201 Fri	7		
	Mon	<b>Tue</b> 28	Decen Wed	nber Thu	201 Fri 1	7 Sat 2	Sun	
	Mon 27 4	<b>Tue</b> 28 5	Decen Wed 29	nber Thu 30 7	201 Fri 1 8	7 Sat 2 9	Sun 3	
	Mon 27 4 11	Tue 28 5 12	Decen Wed 29 6	nber Thu 30 7 14	201 Fri 1 8 15	7 <b>Sat</b> 9 16	Sun 3 10 17 24	
	Mon 27 4 11	Tue 28 5 12 19	Decen Wed 29 6 13	nber Thu 30 7 14 21	201 Fri 1 8 15 22	7 2 9 16 23	Sun 3 10 17 24	
	Mon 27 4 11 18	Tue 28 5 12 19 26	Decen Wed 29 6 13 20	nber Thu 30 7 14 21 28	201 Fri 1 8 15 22	7 2 9 16 23 30	<b>Sun</b> 3 10 17	
	Mon 27 4 11 18 25 1	Tue 28 5 12 19 26	Decen Wed 29 6 13 20 27 3	nber Thu 30 7 14 21 28	201 Fri 1 8 15 22 29 5	7 2 9 16 23 30	Sun 3 10 17 24 31 7	
	Mon 27 4 11 18 25 1	Tue 28 5 12 19 26 2	Decen 29 6 13 20 27 3 227 3	nber Thu 30 7 14 21 28	201 Fri 1 8 15 22 29 5	7 2 9 16 23 30 6	Sun 3 10 17 24 31 7	

Confirm the entered values and generate key pair by clicking on *Create Key*.

			?	×
← Key Pair Creat	ion Wizard			
Review Para	meters			
Please review the	e parameters before proceeding.			
Name:	Example Key Creation			$\sim$
	example@thefake.site			
	RSA			
Key Strength:	2048 bits			
	Encrypt, Sign			
Subkey Type:				
Subkey Strengt				
Subkey Usage:				
Valid Lintil				¥
Show all deta	ls			
	1	-		
	1		6	-1
		Create	Cano	ei

Enter a password that you remember for your private key. This password will be used to decrypt the files that you receive encrypted with your public key.



Clicking **OK** you will see your public / private key pair have been generated correctly.

Asistente de creación del par de claves

#### Par de claves creado correctamente

Su nuevo par de claves se ha creado correctamente. Consulte los detalles sobre el resultado y algunos pasos a seguir sugeridos más abajo.

Par de claves crea Huella digital: 0A9			AB4FBBA7E0	C0E342		
liquientes pasos						
	Ha	cer copia de	respaldo de s	su par de clave	s	
		Enviar cla	ave pública p	or correo		
	Envi	iar clave públ	lica a un serv	vicio de directo	rio	
					-	

You can check your certificates in the tabs *My Certificates*.

						certificado	13/07/2	021 12//	07/2023	AB4F BBA
	Nombre			(	orreo	ID de los usua	arios Válido d	esde Váli	do hasta	ID de la clave
Buscar <alt< th=""><th>+Q&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>Todos los</th><th>s certificados</th></alt<>	+Q>								Todos los	s certificados
mar/Cifrar	Descifrar/verificar	Importar	Exportar	Certificar	Q Búsqueda en el servidor	ET Certificados	E Bloc de notas	SmartCard	ls	
hivo Ver			Preferencias	Ventana	Ayuda			-		
										-

### Export the public key

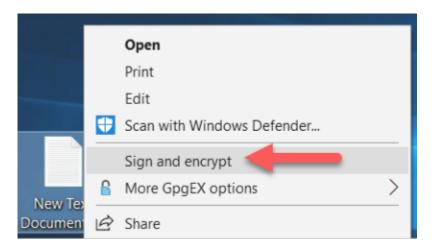
When exporting the public key a text file is generated. As a general rule, it is saved with the extension *.asc*. You can send this file by email or publish it on a public key server as *REDIRIS* where anyone can download it.

Nombre	9			Correo				
Sherlock Holmes								
	<b>E</b>	Certificar						
		🖅 Revocar certificación						
		Certificado raíz	de confianza					
		Certificado raíz	no de confiar	nza				
		Cambiar la con	fianza de la ce	ertificación				
		Cambiar la fect	na de vencimie	ento				
		Cambiar la fras	e de contrase	ña				
		Agregar ID de	usuario					
	Û	Borrar			Del			
		Exportar			Ctrl+E			
		Copia de respa	ldo de las clav	/es secretas				

You will get a file of this type :

Sherlock
Holmes_0xB9620
E06_public

Encrypt files with the public key.



#### Decrypt files with private key

Only if a \* .gpg \* file has been encrypted with your public key and has the private key as well as your password, will you be able to decrypt its content .

You can use the context menu *Decrypt and verify* to recover the original file. It is also possible to do this from the Kleopatra.

		Open
	۲	Run as administrator
		Troubleshoot compatibility
		Pin to Start
		Scan with Windows Defender
		Sign and encrypt
Decrypt	8	More GpgEX options
Verify	Ŀ	Share
Decrypt and verify	1-	Give access to
Encrypt		Pin to taskbar
Sign		
Sign and encrypt		Restore previous versions
Import keys		Send to
Create checksums	-	Cut
Verify checksums		Сору
Help on GpgEX	_	Create shortcut
About GpgEX		Delete
		Rename
		Properties

It will have the same name without the gpg extension.



IMPORTANT NOTE: If you change computers or use a different one, make sure you have your key pair in a safe place. Without them you will not be able to decrypt the content of the file. Therefore, we recommend making a backup of the GPG key pair