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.

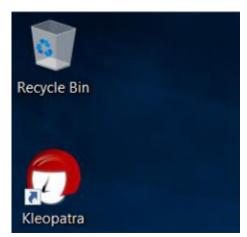
It consists of several modules, including:

- 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

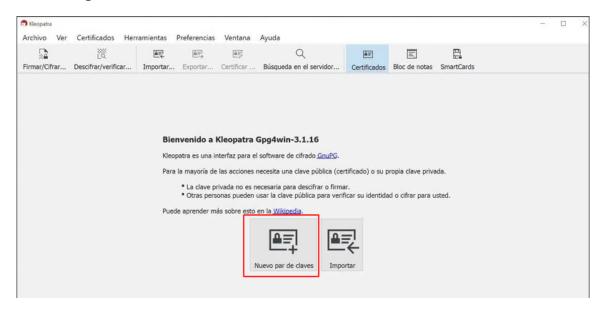
On the project website download the latest version of the software. Open the installer and authorize the changes if necessary. Follow the steps indicated with the Next button.

🔒 Gpg4win Setup			_		\times
Gpg4win	Welcom Gpg4wi		installation	of	
GnuPG for Windows	file encryptio Windows, Bo supported, O	n using the cor th relevant cry penPGP and S/	age for Windows e component Gnu ptography standa MIME. Gpg4win a Iwin is Free Softw	IPG for rds are and the	and
$-\mathbf{O}$	Click Next to	continue.			
	This is Gpg41 Release date	vin version 3.1. 2018-08-31	3		
			Next >	Can	icel
🔒 Gpg4win Setup 🛛 🖑			_		×
1.1	hoose Compo Choose which fea		vin you want to i	nstall.	
Check the components you w install. Click Next to continue.		uncheck the co	mponents you do	on't want t	to
Select components to install:	GnuPG Kleopatra GPA GpgOL GpgEX Browser int	egration	Description Position your over a comp see its descr	onent to	
Space required: 98.2MB					
Gpg4win-3.1.3		. Bard	No. 4		
		< Back	Next >	Cano	cel



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.

	ar un par de claves personales OpenPGP ares de claves OpenPGP están certificados por la confirmación d pública.	le la huella di	gital de la
Los p	ar un par de claves personales X.509 y una petici ares de claves X.509 se certifican por una autoridad de certificac rada necesita enviarse a la CA para finalizar la creación.		
		Next	Cancel
nter the red	quired data		
Introdu Por favor	de creación del par de claves JZCA detalles , introduzca sus detalles personales debajo. Si desea más control sobre onfiguración avanzada».	los parámetros	5, pulse el
Introdu Por favor botón «C	uzca detalles , introduzca sus detalles personales debajo. Si desea más control sobre	los parámetros	
Introdu Por favor botón «C	uzca detalles , introduzca sus detalles personales debajo. Si desea más control sobre onfiguración avanzada».	los parámetros	(opcional
Por favor botón «C Nombre:	uzca detalles , introduzca sus detalles personales debajo. Si desea más control sobre onfiguración avanzada».	los parámetros	(opcional
Por favor botón «C Nombre:	uzca detalles , introduzca sus detalles personales debajo. Si desea más control sobre onfiguración avanzada». Julián G.	los parámetros	s, pulse el (opcional) (opcional)
Por favor botón «C Nombre:	uzca detalles , introduzca sus detalles personales debajo. Si desea más control sobre onfiguración avanzada». Julián G. Proteger la clave generada con una frase de contraseña.		(opcional)

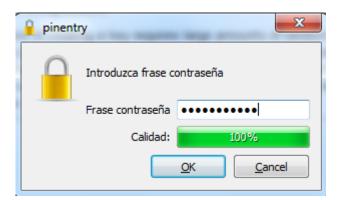
In the *Advanced Settings* tab, indicate a 4096 bits key length and an expiration date no more than 2 years.

🗊 Advanced Settir	ngs						?	×
Technical Details								
Key Material								
	4,0	096 bit	s		•			
▼ +RSA	4,0	096 bit	s		•			
C DSA	2,0)48 bit	s (defa	ult)	~			
F + Elgame	al 2,0	048 bit	s (defa	ult)	Ψ.			
Certificate Usage								
Signing			M	Certific	ation			
Encryption					P			
I∾ Encrypuon				Authen	ticatio	n		
	2017-	12-31	(Authen	ticatio		€3 ▼	
	2017-		Decen	_	_		€] ▼	
	2017- Mon			nber	201			
			Decen Wed	nber	201 Fri	7		
	Mon	Tue 28	Decen Wed	nber Thu	201 Fri 1	7 Sat 2	Sun	
	Mon 27 4	Tue 28 5	Decen Wed 29	nber Thu 30 7	201 Fri 1 8	7 Sat 2 9	Sun 3	
	Mon 27 4	Tue 28 5 12	Decen Wed 29 6	nber Thu 30 7 14	201 Fri 1 8 15	7 <mark>Sat</mark> 2 9 16	Sun 3 10	
	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	Sun 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 Wed 29 6 13 20 27 3 2-31	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*.

			?	×
← к	ey Pair Creatio	on Wizard		
Re	view Parar	neters		
Plea	ase review the	parameters before proceeding.		
Na	ame:	Example Key Creation		^
En	nail Address:	example@thefake.site		
Ke	ey Type:	RSA		
Ke	ey Strength:	2048 bits		
Us	sage:	Encrypt, Sign		
Su	ubkey Type:	RSA		
Su	ubkey Strength	: 2048 bits		
Su	ubkey Usage:	Encrypt		
Va	alid Until	Friday October 2, 2020		~
	Show all details	s		
		1		_
		Create	Can	cel

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.

Huella digital: 0A97759CC8	4026BD56749920A	B4FBBA7E0C0E34	42	
Siguientes pasos				
	Hacer copia de re	espaldo de su par	de claves	
	Enviar cla	ve pública por cor	reo	
	Enviar clave públi	ca a un servicio d	e directorio	

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

Julián						certificado	13/07/2	021 13/0	07/2023	AB4F BBA
-	Nombre			0	orreo	ID de los usua	arios Válido d	esde Váli	ido hasta	ID de la clave
Buscar <alt< th=""><th>+0></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>Todos los</th><th>s certificados</th></alt<>	+0>								Todos los	s certificados
Firmar/Cifrar	Descifrar/verificar	画. Importar	Exportar	Certificar	Q Búsqueda en el servidor	AT Certificados	E Bloc de notas	SmartCard	is	
rchivo Ver		rramientas	Preferencias	Ventana	Ayuda					

Export the public key

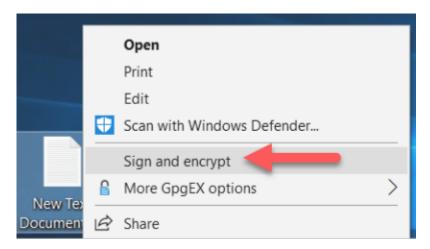
When exporting the public key a text file is generated. As a general rule, it is saved with the extension *.asc*. You can send this file by email or publish it on a public key server as *REDIRIS* where anyone can download it.

Nombre		Correc	D					
Sherlock Holmes								
E	Certificar							
(A1)	Revocar certific	Revocar certificación						
	Certificado raíz	z de confianza						
	Certificado raíz	z no de confianza						
	Cambiar la con	nfianza de la certificación						
	Cambiar la fecl	ha de vencimiento						
	Cambiar <mark>la</mark> fras	se de contraseña						
	Agregar ID de	usuario						
t	Borrar		Del					
	Exportar		Ctrl+E					
	Copia de respa	aldo de las claves secretas						

You will get a file of this type :



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
		•	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	-	Give access to
	Encrypt		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
	Sign		Pin to taskbar
	Sign and encrypt		Restore previous versions
	Import keys		Send to
	Create checksums	-	Cut
	Verify checksums		Сору
	Help on GpgEX	-	Create shortcut
	About GpgEX		Delete
1			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