¿ Qué es GPG ?

Ver descripción aquí

GPG para usuarios windows

Existen varias aplicaciones bajo el sistema operativo Windows que permiten generar un par de claves gpg. Entre las más conocidas está Gnu4win y su módulo [Kleopatra]. La aplicación Gpg4win es un software de encriptación de libre distribución el cual permite el cifrado de ficheros y el envío de documentos a través del correo electrónico utilizando criptografía de clave pública para el cifrado de datos y firmas digitales.



Soporta los estándares de criptografía OpenPGP y S/MIME (X.509).

Gpg4win se compone varios módulos, entre ellos:

- GnuPG : la herramienta de cifrado básico
- Kleopatra : administrador de certificados para OpenPGP y X.509
- + GPA : un administrador de certificados alternativa (${\rm GNU}$) para OpenPGP y X. 509

Instalación de GPG4win

En la web del proyecto descargar la versión más reciente del software. Abrir el instalador y autorizar los cambios en caso necesario. Seguir los pasos indicados con el botón Siguiente.

🔒 Gpg4win Setup		_		\times
Gpg4win	Welcome to the in Gpg4win	stallatior	n of	
GnuPG for Windows	Gpg4win is an installer packag file encryption using the core of Windows. Both relevant crypto supported, OpenPGP and S/MJ software included with Gpg4w Click Next to continue.	ie for Windows component Gnu ography standa IME. Gpg4win a in is Free Soft	s for EMail uPG for rds are and the ware.	and
	This is Gpg4win version 3.1.3 Release date 2018-08-31			
		Next >	Car	ncel
🔒 Gpg4win Setup 🛛 🖑		_		×
Gpg4win	hoose Components Choose which features of Gpg4wir	n you want to i	nstall.	
Check the components you we install. Click Next to continue.	ant to install and uncheck the com	ponents you de	on't want	to
Select components to install:	 ✓ GnuFG ✓ Kleopatra GPA ✓ GpgOL ✓ GpgEX Browser Integration 	Description Position you over a comp see its descr	r mouse conent to ription.	
Space required: 98.2MB				
Gpg4win-3.1.3	< Back	Next >	Can	cel



Generar una par de claves (pública y privada)

Una vez instalado Gpg4win vamos a utilizar el módulo **Kleopatra** para generar un nuevo par de claves gpg. Para ello desde la pestaña *Archivo* seleccionamos *Nuevo Certificado*, lo cual abrirá el asistente de generación de certificados.



Pulsa en Nuevo par de claves GPG

Asistente de creación del par de claves

Elegir formato

Por favor, elija qué tipo quiere crear.

clave	pública.	estan certificados por la co	onfirmación de la huella d	ligital de la
→ Crea Los p gene	ar un par de claves ares de claves X.509 se ce rada necesita enviarse a la	personales X.509 y ertifican por una autoridad a CA para finalizar la creac	una petición de cei l de certificación (CA). La ión.	tificación ^{petición}
			Next	Cancel
troducir l	os datos requeridos			
- Asistente	de creación del par de claves			
Introdu Por favor botón «C	IZCA detalles introduzca sus detalles pers onfiguración avanzada».	sonales debajo. Si desea más	control sobre los parámetro	os, pulse el
Por favor botón «C Nombre:	IZCA detalles introduzca sus detalles personfiguración avanzada». Julián G.	sonales debajo. Si desea más	control sobre los parámetro	os, pulse el
Por favor botón «C Nombre: Correo:	uzca detalles introduzca sus detalles personfiguración avanzada». Julián G.	sonales debajo. Si desea más	control sobre los parámetro	os, pulse el (opciona (opciona
Por favor botón «C Nombre: Correo:	uzca detalles introduzca sus detalles personfiguración avanzada». Julián G. Proteger la clave genera	sonales debajo. Si desea más da con una frase de contrase	control sobre los parámetro ña.	os, pulse el (opciona (opciona
Por favor botón «C Nombre: Correo:	uzca detalles introduzca sus detalles personfiguración avanzada». Julián G.	sonales debajo. Si desea más da con una frase de contrase Julián G.	control sobre los parámetro ña.	os, pulse el (opciona (opciona
Introdu Por favor botón «C Nombre: Correo:	uzca detalles introduzca sus detalles per onfiguración avanzada». Julián G. Proteger la clave genera	sonales debajo. Si desea más da con una frase de contrase Julián G.	nña. Configura	os, pulse el (opciona (opciona

En la pestaña *Avanzadas* indicar una longitud de clave de 4096 bits y una fecha de caducidad en el desplegable inferior no superior a 2 años.

n Advanced Setti	ngs						?	×
Technical Details	1							
Mary Markey and								
Key Material								
BSA	4,0	096 bit	s		•			
✓ +RSA	4.0	096 bit	s		-			
6				143	-			
C <u>D</u> SA	2,0	048 bit	s (deta	ult)	Ψ.			
F + Elgama	al 2,0	048 bit	s (defa	ult) _	Ψ.			
Certificate Usage	•							
Signing			되	Certific	ation			
E -			_					
Encryption				A men		-		
1. Eng (1900)				Control	1000100			
Valid until:	2017-	12-31		Guarden			€3 ▼	
Valid until:	2017-	12-31	Decen	nber	201	7	€3 ▼	
Valid until:	2017-	12-31 Tue	Decen	nber Thu	201 Fri	7 Sat	€3 - Sun	
Vald until:	2017- Mon	12-31 Tue	Decen Wed	nber Thu 30	201 Fri	7 Sat	Sun	
Vald until:	2017- Mon 27 4	12-31 Tue 28 5	Decen Wed 29 6	nber Thu 30 7	201 Fri 1 8	7 5at 2 9	€ ▼ Sun 3 10	
Vald until:	2017- Mon 27 4 11	12-31 Tue 28 5 12	Decen Wed 29 6 13	nber Thu 30 7 14	201' Fri 1 8 15	7 Sat 2 9 16	Sun 3 10 17	
Vald until:	2017- 27 4 11 18	12-31 Tue 28 5 12 19	Decen Wed 29 6 13 20	nber Thu 30 7 14 21	201 Fri 1 8 15 22	7 <u>Sat</u> 9 16 23	Sun 3 10 17 24	
V Vald until:	2017- 27 4 11 18 25	12-31 Tue 28 5 12 19 26	Decen Wed 29 6 13 20 27	nber Thu 30 7 14 21 28	201 ¹ Fri 1 8 15 22 29	7 2 9 16 23 30	Sun 3 10 17 24 31	
Vald unti:	2017- 27 4 11 18 25 1	12-31 28 5 12 19 26 2	Decen Wed 29 6 13 20 27 3	nber Thu 30 7 14 21 28 4	201' Fri 1 8 15 22 29 5	7 2 9 16 23 30 6	Sun 3 10 17 24 3 7	
Vald until:	2017- 27 4 11 18 25 1	12-31 Tue 28 5 12 19 26 2 2017-1	Decen Wed 29 6 13 20 27 3 2-31	nber Thu 30 7 14 21 28 4	201 Fri 1 8 15 22 29 5	7 2 9 16 23 30 6 Veck 5	Sun 3 10 17 24 3 7 2	
Vald until:	2017- 27 4 11 18 25 1	12-31 Tue 28 5 12 19 26 2 2017-1	Decen 29 6 13 20 27 3 2-31	nber Thu 30 7 14 21 28 4	201 Fri 1 8 15 22 29 5	7 2 9 16 23 30 6 Veek 5	Sun 3 10 17 24 3 7 2 2 •	
Vald until	2017- 27 4 11 18 25 1 Ne	12-31 28 5 12 19 26 2 2017-1 oxt Yea	Decen Wed 29 6 13 20 27 3 2-31 r	nber Thu 30 7 14 21 28 4	201 Fri 1 8 15 22 29 5 V	7 2 9 16 23 30 6 /eek 5	Sun 3 10 17 24 3 7 2 2	

Confirmar los valores introducidos y generar las claves pulsando en *Crear*.

				?	×
÷	Key Pair Creati	on Wizard			
I	Review Parar	neters			
1	Please review the	parameters before proceeding.			
	Name:	Example Key Creation			\sim
	Email Address:	example@thefake.site			
	Key Type:	RSA			
	Key Strength:	2048 bits			
	Usage:	Encrypt, Sign			
	Subkey Type:	RSA			
	Subkey Strength	: 2048 bits			
	Subkey Usage:	Encrypt			
	Valid Until-	Eriday October 2 2020			~
	Show all detail	s			
		1			
			Create	Canc	el

Introducir una contraseña que recuerde para su clave privada. Esta contraseña será la que deba usar para descrifrar los archivos que reciba cifrados con su clave pública.



Al pulsar **OK** verá que su par de claves pública/privadas se han generado correctamente

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: 0A	97759CC84026	ente. BD56749920AE	4FBBA7E0C0E	342	
liquientes pasos					
	Had	cer copia de re	spaldo de su p	ar de claves	
		Enviar clave	e pública por c	orreo	
	Envi	iar clave públic	a un servicio	de directorio	

Se puede comprobar que se han creado con éxito el par de claves en la pestaña *Certificados.*

Importar Emp Emp Emp Emp Importar Descifrar/verificar Importar Exportar Certificados Bloc de notas SmartCards Buscar< <alt+0> Todos los certificados Todos los certificados Todos los certificados Nombre Correo ID de los usuarios Válido desde Válido hasta ID de la clave</alt+0>	rchivo Ver Certificados Herramientas Preferencias Ventana Ayuda Image: Control Image: Certificar Image: Certificar Image: Certificar Image: Certificados Image: Ce	Buscar <alt< th=""><th>+0> Nombre</th><th></th><th></th><th>c</th><th>orreo</th><th>ID de los usua</th><th>arios Válido d</th><th>esde Válie</th><th>do hasta</th><th>ID de la clave</th></alt<>	+0> Nombre			c	orreo	ID de los usua	arios Válido d	esde Válie	do hasta	ID de la clave
Image: Control of the second secon	rchivo Ver Certificados Herramientas Preferencias Ventana Ayuda Image: Construction Image: Certification Image: Certification </th <th>Buscar<alt< th=""><th>+Q></th><th></th><th></th><th></th><th></th><th></th><th></th><th>1</th><th>10000100</th><th></th></alt<></th>	Buscar <alt< th=""><th>+Q></th><th></th><th></th><th></th><th></th><th></th><th></th><th>1</th><th>10000100</th><th></th></alt<>	+Q>							1	10000100	
Imar/Cifrar Descifrar/verificar Importar Exportar Exportar <th>rchivo Ver Certificados Herramientas Preferencias Ventana Ayuda</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>Todos los</th> <th>s certificados</th>	rchivo Ver Certificados Herramientas Preferencias Ventana Ayuda										Todos los	s certificados
	rchivo Ver Certificados Herramientas Preferencias Ventana Ayuda	mar/Cifrar	Descifrar/verificar	Importar	Exportar	Certificar	Q Búsqueda en el servidor	ET Certificados	E Bloc de notas	SmartCard	s	

Exportar la clave pública

Al exportar la clave pública se genera un fichero de texto que por norma general se almacena con la extensión *.asc,* que es el que podrá distribuir por correo electrónico o bien publicar en un servidor de claves públicas como *REDIRIS* y donde cualquier persona la puede descargar.

Nom	ore		Correo
Sherlock Holmes			
	E	Certificar	
		Revocar certificación	
		Certificado raíz de conf	fianza
		Certificado raíz no de c	onfianza
		Cambiar la confianza d	e la certificación
		Cambiar la fecha de ve	ncimiento
		Cambiar la frase de cor	ntraseña
		Agregar ID de usuario	
		Borrar	Del
	Þ	Exportar	Ctrl+E
		Copia de respaldo de la	as claves secretas

Obtendrá un fichero de este tipo:

Sherlock
Holmes_0xB9620
E06_public

Cifrar ficheros con la clave pública.



Descifrar ficheros con la clave privada

Sólo si un archivo *.gpg* ha sido cifrado con su clave pública y tiene la clave privada, así como su contraseña, podrá descifrar su contenido.

Se puede usar el menú contextual *Descifrar y verificar* para recuperar el fichero original pulsando con el segundo botón. También es posible realizar esto desde Kleopatra.

	Open
	💎 Run as administrator
	Troubleshoot compatibility
	Pin to Start
	Scan with Windows Defender
	Sign and encrypt
Decrypt	More GpgEX options
Verify	년 Share
Decrypt and verify	Cive access to
Encrypt	Dire access to
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
	Rename
	Properties

Una vez desencriptado este tendrá el mismo nombre sin la extensión gpg.



NOTA IMPORTANTE: Si cambia de ordenador o usa uno diferente asegurese de tener su par de claves a buen recaudo. Sin ellas no tendrá la posibilidad de descrifrar el contenido del archivo. Por ello recomendamos realizar un backup del par de claves GPG