

Asistente de uso de PGP

sólo Este manual abreviado comprende varias secciones. Pulse sobre la sección que le interese, o examínelas todas consecutivamente si desconoce el manejo de PGP y desea alcanzar en pocos minutos un nivel aceptable en la utilización del programa.

1. Configuración de PGP
2. Manejo de claves
3. Aspecto de los mensajes cifrados y/o firmados
4. Cifrar/firmar mensajes desde el icono PGP
5. Descifrar/verificar mensajes desde el icono PGP
6. Cifrar/firmar mensajes desde el programa de correo
7. Descifrar/verificar mensajes desde el programa de correo
8. Cifrar/firmar ficheros desde el Explorador de Windows
9. Descifrar/verificar ficheros desde el Explorador de Windows
10. Borrado seguro de ficheros desde el Explorador de Windows
11. Convertirse en usuario avanzado

Configuración de PGP

Una vez haya instalado PGP correctamente, deberá aparecer

un

nuevo icono, representando un candado, en su barra de tareas (ver figura). Ese es el icono de PGP, que le permitirá acceder a todas las funciones del programa y que, a partir de ahora, estará presente cada vez que arranque Windows.

Si pulsa sobre ese icono con el botón derecho del ratón, se desplegará el menú que muestra la figura de la izquierda. Sitúe el cursor del ratón sobre "Options", tal y como se indica, y pulse una vez el botón izquierdo.

Al hacerlo, aparecerá la pantalla de configuración de PGP, que dispone de varias pestañas. Asegúrese de que la primera pestaña (etiquetada como "General") aparezca idéntica a la

que le

mostramos. La única excepción es el recuadro opcional

"Comment

Block", donde usted puede incluir cualquier mensaje breve

que

desea que aparezca en todos sus mensajes firmados o

cifrados.

Es aconsejable que lo utilice para indicar el método (URL,

petición

por e-mail, etc) por el que el receptor de su mensaje puede obtener su clave para comunicarse con usted. Es muy

importante

que aparezca activada la casilla "Always Encrypt to default key", lo que le permitirá poder descifrar sus propios

mensajes

cuando lo necesite.

le
etiquetada

PGP

una

que

70

ejemplo).

no

invalidaría

hecho, es

defecto (al

se

Vamos ahora a la tercera pestaña, etiquetada "Email". Como

mostramos, la única casilla que conviene activar es la

como "Word-wrap clearsigned messages at column...". En ese espacio debe usted teclear la longitud de línea a la que

deberá recortar sus mensajes. ¿Qué número poner ahí? Hay

regla que no falla: un número varias unidades menor que el

tenga usted configurado en su programa de correo. Así, 69-

70 puede ser una buena opción si su programa de correo está configurado para cortar las líneas a 74 caracteres (por

De ese modo, nos aseguramos de que el programa de correo

vuelva a recortar el mensaje firmado con PGP, lo que

la firma (más sobre esto más adelante).

Como resulta evidente, existen muchas más opciones por configurar, pero no es imprescindible hacerlo ahora. De

posible que nunca necesite modificar las opciones por

menos, nunca antes de haberse leído el manual del programa para saber muy bien lo que hace).

Breve introducción teórica

Si se acuerda, durante la instalación usted generó sus propias claves PGP. Hablamos en plural porque se trata de un par de claves, relacionadas de tal forma que lo que se cifra con una

descifra con la otra. No obstante, y a todos los efectos,

la
PGP usted

clave
carpeta
SECRING
claves (y,
irá
que usted
sus
públicas de
validez de
2)

necesita la
ellos
Por tanto,
SER
COLECCIONADAS. No

hablaremos de dos claves diferentes: su clave SECRETA y clave PÚBLICA. (No se preocupe: tras la instalación de ya dispone de ambas).

Cada una de esas dos claves está contenida en un fichero diferente: la clave secreta reside en SECRING.SKR y la pública en PUBRING.PKR (ambos ficheros están en una carpeta del directorio donde instaló PGP). Mientras el fichero permanecerá idéntico mientras usted no genere nuevas claves (y, en principio, no necesita hacerlo), el fichero PUBRING irá incrementando progresivamente su tamaño a medida que usted vaya recopilando las claves públicas que le proporcionan sus interlocutores. ¿Y para qué necesita usted las claves públicas de sus interlocutores? Para dos cosas: 1) poder verificar la validez de los mensajes firmados digitalmente que otros le envíen, y 2) poder enviarles a ellos mensajes cifrados.

Algo debe quedar muy claro desde el principio: usted necesita la clave pública de otros para poder cifrarles mensajes, y ellos necesitan la suya para poder hacer lo propio con usted.

LAS CLAVES PÚBLICAS ESTÁN DESTINADAS A SER INTERCAMBIADAS, TRANSMITIDAS Y

debe usted tener ningún reparo en poner su clave pública en su web, enviársela a todo el que se la pida o publicarla en un servidor de claves (un ordenador de libre acceso que contiene una colección de claves muy, muy grande). Incluso podría publicarla en el diario de la mañana sin ningún perjuicio para usted (de hecho, cuando más se difunda su clave pública menos posibilidades habrá de suplantar su identidad en la Red).

Con la misma rotundidad de la afirmación anterior, le hago esta:

SU SEGURIDAD RESIDE EN QUE SU CLAVE SECRETA NO ESTÉ AL ALCANCE ABSOLUTAMENTE DE NADIE. Por tanto, no debe usted dejarla en un ordenador que utilicen otros (mejor copiéla en un disquete que nunca abandone). Su clave secreta (fichero SECRING.SKR, ¿recuerda?) está siempre protegida mediante contraseña (la que usted utilizó en la instalación de PGP y que puede cambiar en cualquier momento). Por tanto, si alguien le roba su fichero SECRING.SKR (o dispone de acceso a él), aún debe descubrir su contraseña antes de poder hacerse con su clave secreta. A partir de ese momento, su seguridad depende sólo de la calidad de la contraseña que eligió. Si no es demasiado

**poco tiempo
como
mensajes
alguien
SECRING.SKR, para
la Red,
anterior.**

**buena, un atacante capaz puede averiguarla en muy
y descifrar todos sus mensajes a partir de entonces, así
suplantarlo en cualquier foro o falsificar su firma en los
de correo. Por tanto, si tiene fundadas sospechas de que
ha accedido a su clave secreta (a su fichero
entendernos) usted debe olvidarse de esa clave, avisar a
generar otra nueva y protegerla mucho mejor que la**

de

**Una vez asimilado todo lo anterior, pasaremos al manejo
claves propiamente dicho.**

**arrancar la
ratón sobre**

**Manejo de claves
Para cualquier operación relativa a sus claves deberá
utilidad PGPKeys. Para ello pulse el botón derecho del
el icono de PGP en la barra de tareas, tal
y como muestra la figura adjunta.**

**momento
cada clave
clave
parámetros de
no es**

**El aspecto de la ventana que se abre es el de la figura. Se
muestran las claves de que usted dispone en cada
(columna "Keys"), junto a dos parámetros propios de
("Validity" y "Trust"), su tamaño ("Size") y el tipo de
("Description"). También es posible mostrar más
cada clave si se seleccionan en el menú "View", pero eso
necesario ahora.**

(PGPKeys)

y

en

más

propia

usuarios

Una ligera exploración por los menús de esta ventana le permitirá observar que hay muchas opciones, operaciones y comandos que es posible utilizar con las claves. No obstante, este curso acelerado nos centraremos en las dos operaciones comunes e imprescindibles para todo usuario: exportar su clave pública e incorporar las claves públicas de otros (ver fundamentos teóricos en la sección anterior).

1. Extraer su propia clave para dársela a otros:

pública

duda.

Como ya sabemos su interlocutor necesita tener la clave de usted para poderle enviar a usted mensajes cifrados (y también para comprobar que la firma digital de usted es correcta). NOTA: Disculpe el abuso del "usted" pero es imprescindible en este contexto para que no quede ninguna

necesita

de

y

Para darle su propia clave a alguien usted necesita antes extraerla de su fichero de claves o, en otros términos, exportarla. Para ello, busque su propia clave en la ventana PGPKeys (normalmente aparecerá en negrita), selecciónela y pulse el botón derecho del ratón. Del menú emergente que aparece seleccione "Export...".

guardar

Al hacerlo, aparecerá el cuadro de dialogo habitual para (o salvar) ficheros. Como nombre de fichero por defecto aparecerá el suyo, y como extensión .ASC

(aparecerán también dos casillas que deben seguir desactivadas). Cuando pulse el botón Aceptar se escribirá en su disco duro el fichero [su_nombre].asc, que incluso dispone de un icono propio como muestra la figura adyacente.

Este fichero contiene su propia clave pública y usted puede remitirlo como adjunto de un correo electrónico a la persona con la que decida comunicarse de forma cifrada. También puede ponerlo a disposición de todo el mundo en su propia página web (si la tiene) o en un ordenador de acceso público que hace de gran almacén de claves públicas (es lo que se denomina servidor de claves (hay varios disponibles en la opción de menú "Server" de la barra de menús de PGPKKeys o en la opción "Send to..." que aparece al pulsar el botón derecho sobre la propia clave. Puede usted añadir otros servidores a través del menú "Options" de PGP, pero no es necesario porque todos los servidores de claves PGP del mundo conforman una gran base de datos distribuidos, de forma que se transmiten la información automáticamente entre ellos y la actualizan, sin que usted tenga que preocuparse del proceso).

Por último, existe otra forma de distribuir su propia clave. Basta con que abra el fichero .ASC con cualquier editor de texto (el bloc de notas de Windows, por ejemplo) y verá que tiene un aspecto como el de la figura. Basta con que copie todo el texto y lo pegue en un mensaje normal de correo para que, al recibirlo, su destinatario pueda disponer de la clave pública de usted.

2. Obtener las claves públicas de otros:

sentido
importar:
(Server

Como puede imaginarse, el proceso es paralelo (pero en inverso) al descrito en el apartado anterior. Ahora usted necesitará importar las claves que otros le envíen, bien desde ficheros adjuntos (haciendo doble click sobre él), bien desde mensajes de correo (copiar, pegar, salvar como .ASC e Keys -> Import) o bien desde servidores de claves PGP -> Search).

en que
cuando
muy
difícil
sirve y

Lo importante aquí es que hasta que usted no disponga de la clave pública de la persona a la que quiere enviar mensajes cifrados, no estará en condiciones de hacerlo. Insistiremos el intercambio de claves públicas no necesita ningún tipo de secreto o cuidado especial: puede hacerse de forma abierta y transparente. Dé su clave pública a todo el que se la pida e incluso publíquela en un servidor de claves, siempre y cuando esté seguro de que se trata de su clave definitiva (si se precipita en publicar claves temporales o de prueba, luego es muy probable que no sea capaz de retirarlas, con lo cual será difícil diferenciar qué clave es la que usted emplea y cuál ya no sirve y no debe emplearse).

FIRMA DE CLAVES

Cuando

Otra operación frecuente es el firmado de claves públicas.

usted firma la clave pública de otra persona, su acción tiene el mismo significado que en el mundo real: usted suscribe que esa clave pertenece a esa determinada persona. De ese modo, otros, que confíen en usted, reconocerán también esa clave como válida, puesto que usted la ha reconocido como tal.

De lo anterior se deduce que usted debe ser cuidadoso a la hora de firmar las claves de otros. De hecho, sólo deberá hacerlo cuando esté absolutamente seguro de que pertenecen a quien afirma ser su propietario.

Una vez decida firmar la clave de otro, la operación es bien sencilla: arranque PGPPKeys, seleccione la clave a firmar, pulse el botón derecho y elija "Sign...". No olvide que para firmar se utiliza su clave secreta, por lo que PGP le pedirá su contraseña a la hora de firmar cualquier clave.

Existe una diferencia fundamental entre utilizar claves firmadas o no firmadas. Cuando usted comprueba un mensaje firmado digitalmente con una clave que usted no ha reconocido firmándola, PGP le informará con el mensaje "Invalid Key". Estas palabras pueden resultar equívocas para usuarios hispanohablantes, ya que no significan que la clave tenga cualquier defecto o que la firma de su interlocutor no sea buena, sino tan sólo que usted no ha validado previamente la clave pública del firmante.

Como es fácil imaginar, las claves de otras personas que usted incorpore a su PGP han podido ser ya firmadas por otras personas

antes que usted. Para ver las firmas que acompañan a una determinada clave arranque PGPKeys y despliegue la clave pulsando sobre el signo + que aparece a su izquierda. Los firmantes de esa clave aparecerán junto a un icono bastante expresivo (ver figura).

una
clave antes de firmarla, que periódicamente se organizan
"sesiones
de firma de claves", donde los participantes se aseguran fehacientemente de la identidad de cada cual y firman sus
claves
públicas en consecuencia.

Aspecto de los mensajes cifrados y/o firmados

Antes de enseñarle cómo se firman y cifran mensajes de
correo
electrónico, consideramos necesario mostrarle cuál es el
aspecto
que muestran ambos tipos de mensajes en la práctica,
cuando se
examinan en cualquier programa de correo.

1. Aspecto de un mensaje firmado

Un mensaje firmado "en claro" (clearsigned) puede leerlo cualquiera (aunque no sea usuario de PGP). El texto
permanece
del mensaje permanece perfectamente legible y la única diferencia con un mensaje normal (no firmado) es que el
texto
aparece delimitado entre un encabezado (BEGIN PGP
SIGNED
MESSAGE) y un bloque final repleto de caracteres que
parecen no
tener ningún sentido (ver figura).

¿Qué sentido tiene pues firmar un mensaje de correo? muy sencillo: las personas que utilicen PGP y dispongan de la clave pública de usted podrán comprobar, de forma inapelable y fehaciente, que ese mensaje ha sido realmente escrito por usted, y no por un impostor. De ese modo, al firmar un mensaje, usted se compromete con su contenido. Adicionalmente, si su mensaje hubiera sido interceptado por alguien, que hubiera cambiado una simple coma, el receptor del mismo (y también usuario de PGP) detectaría de inmediato la manipulación. De ese modo, al firmar "en claro" sus mensajes, usted obtiene la garantía adicional de que sus mensajes no pueden ser manipulados por nadie sin que se note.

2. Aspecto de un mensaje cifrado

Por el contrario, en un mensaje cifrado es absolutamente imposible reconocer el texto del mensaje a cualquier persona que no sea su legítimo destinatario (es decir, la persona cuya clave pública usted utilizó para cifrarlo). (ver figura)

Por tanto, para recuperar el texto original del mensaje, su destinatario debe ser también usuario de PGP y usted ha debido cifrarlo para él.

NOTA: Firmar y cifrar mensajes no son operaciones

concluyentes. Usted puede efectuar ambas operaciones a la vez sobre el mismo mensaje, obteniendo a la vez dos ventajas: confidencialidad (ningún extraño puede leerlo) y autenticidad (usted demuestra ser su autor). También existe la garantía de no manipulación del mensaje. El aspecto de un mensaje firmado y cifrado a la vez es indiferenciable a simple vista del de un mensaje sólo cifrado.

Cifrar/firmar mensajes desde el icono PGP

Más adelante veremos que firmar y cifrar mensajes resulta mucho más cómodo cuando nuestro programa de correo habitual que de que de habrá soporte puede obstante, le utiliza PGP pero que está disponible en toda circunstancia).

Si PGP no le ofreción instalar un módulo para su programa de correo, aún puede cifrar y firmar mensajes, a través del portapapeles de Windows y el icono de PGP que aparece en la barra de tareas. Una vez haya escrito su mensaje, de la manera

habitual, resáltelo entero mediante el ratón (o "seleccionar todo") y copiélo al portapapeles. Pulse ahora sobre el icono de PGP y seleccione "Clipboard" (portapapeles). Las opciones disponibles son "Sign" (firma en claro), "Encrypt" (cifrar) y "Encrypt and Sign" (firmado y cifrado combinado). Seleccione la opción que le interese (recuerde las diferencias).

Cuando seleccione "Sign", PGP le pedirá su contraseña, para poder acceder a su clave secreta (la utilizada para firmar). Cuando seleccione "Encrypt" aparecerá un cuadro para que seleccione la clave pública del destinatario del mensaje (si no aparece ya como seleccionada, haga doble click sobre ella o arrástrela a la ventana inferior). No hay ningún inconveniente en que seleccione varias claves para un mismo mensaje, si los destinatarios van a ser varios.

NOTA: si usted configuró PGP siguiendo nuestras indicaciones, su propia clave debe aparecer como preseleccionada; de ese modo usted también podrá leer los mensajes que cifre para otros.

Cuando haya finalizado, pulse Aceptar (OK). El mensaje firmado (y/o cifrado) pasará inmediatamente al portapapeles de Windows.

La única operación que le queda es volver a su programa de correo, pegar el mensaje cifrado y/o firmado en lugar del texto original y enviar el mensaje a su(s) destinatario(s).

opción

NOTA: Observe que al pulsar sobre el icono PGP, junto a la

utilizar esa

"Clipboard", parece también otra rotulada como "Current Window" (ventana actual). En muchas circunstancias,

del

opción le permite evitar el proceso de copiar/pegar a través

correo

portapapeles. Pruebe si esa opción funciona bien en su caso, porque no siempre lo hace (la ventana de su mensaje de

Descifrar/verificar mensajes

ha de estar en primer plano).

desde el icono PGP

El proceso a seguir para descifrar los mensajes cifrados que reciba, o verificar la firma de los mismos, es idéntico al

descrito

en la sección anterior, salvo que ahora deberá seleccionar, desde el icono de PGP, la opción "Decrypt and Verify" (descifrar y verificar).

ya

Ahora se le pedirá su contraseña para descifrar los mensajes, que PGP necesita acceder a su clave secreta.

Cifrar/firmar mensajes desde el programa de correo

por

Si su programa de correo está soportado mediante módulos

usted está

PGP (algo que debió configurar durante la instalación),

de

en el mejor de los mundos. Su programa de correo dispondrá

de

botones específicos para usar PGP (u opciones de menú) que le permitirán firmar mensajes, cifrarlos, verificar firmas o descifrarlos, a golpe de ratón. También es muy posible que disponga de botones (o menús) para acceder a la utilidad

de

manejo de claves, para incorporar nuevas claves a su PGP,

etc,

etc.

como
manejo

A modo de ejemplo, le presento los botones de PGP tal y aparecen en Microsoft Outlook 98/2000, y las opciones de menú para PGP en el programa de correo The Bat!. Su es evidente, aunque debería usted repasar los conceptos fundamentales sobre claves, firmado y cifrado que hemos expuesto en secciones anteriores.

Cifrar/firmar ficheros desde el Explorador de Windows

de

Por fortuna, PGP no está limitado a cifrar y firmar mensajes de correo o simple texto. También es posible realizar idénticas operaciones sobre cualquier tipo de archivo que se le pueda ocurrir (DOC, XLS, MP3, JPG, AVI, etc, etc...).

Explorador de
del
y/o

El método a seguir es tan sencillo como arrancar el Windows, seleccionar el fichero y pulsar el botón derecho del ratón. Aparecerá una opción de menú que le permitirá cifrar o firmar el fichero:

Cuando se selecciona cifrar un fichero aparece un cuadro de opciones que merece alguna aclaración.

clave
que

En principio, PGP opta por cifrar el fichero mediante la clave pública de un destinatario (que debe ser usted mismo, si lo

proceso es
necesitará la
desea

planea es guardarlo en su ordenador). En ese caso, el
idéntico al descrito para mensajes de correo y usted
contraseña que protege su clave secreta PGP sólo cuando
descifrarlo.

correspondiente

Pero también es posible marcar la casilla "Conventional
Encryption" para proteger el fichero mediante un algoritmo
simétrico (la misma clave cifra y descifra) y la
contraseña que usted seleccione (y que deberá recordar). Si
activa también la casilla "Self Decrypting Archive" obtendrá
además un fichero "autoejecutable", es decir, que sólo con
pulsar
casilla
segura y

sobre él le solicitará la contraseña. Si marca también la
"Wipe original" el fichero original es borrado de forma
definitiva, y sólo permanecerá en su disco la versión cifrada.

¿Y para qué firmar un fichero?

del
validar.

Firmar un fichero permite detectar cualquier modificación
mismo, ya que la firma digital deja inmediatamente de

Por tanto, se trata de un mecanismo bastante habitual para
garantizar la integridad original de ciertas distribuciones de
software.

un

Cuando seleccione la opción firmar desde el explorador de
Windows, se le pedirá su contraseña y se le presentará antes
un
cuadro que contiene la opción "Detached Signature". Si se
selecciona, se obtendrá un fichero de firma separado (pero

original y el estrechamente ligado) del fichero original. El fichero
por fichero de firma se distribuirán juntos (en un mismo ZIP,
usuario de ejemplo, añadiendo también la clave pública del autor,
adecuadamente firmada por otros, para que cualquier
PGP pueda verificar que se trata del fichero original, no
manipulado).

Descifrar/verificar ficheros

desde el Explorador de Windows
El proceso es idéntico al descrito en la sección anterior.
La única diferencia estriba en que cuando usted selecciona
desde el Explorador de Windows un fichero previamente cifrado,
las opciones que se presentarán bajo el menú PGP, al presionar
con el botón derecho, serán distintas: tan sólo "Decrypt and
Verify" y "Wipe".

Borrado seguro de ficheros
desde el Explorador de Windows
Es sabido que borrar un fichero de la forma habitual (opción
"borrar" del Explorador de Windows, por ejemplo) no
elimina por completo el fichero, existiendo multitud de utilidades que
cualquier intruso podría utilizar para recuperar el fichero original.

seguro de

Para evitar eso, PGP incluye un mecanismo de borrado de ficheros ("wipe", en inglés).

más

Se puede acceder a ella desde el explorador de Windows, sin que seleccionar el fichero a borrar, pulsar el botón derecho, seleccionar PGP y luego "Wipe":

(Options -

Usted incluso puede seleccionar el número de pasadas que realizará la opción wipe en el menú de configuración General - File wiping) de PGP.

más

Adicionalmente, PGP incluye una utilidad de borrado aún potente que la anterior. Se trata del borrado de espacio libre ("Free Space Wiper"), que usted puede arrancar desde una utilidad que aún no hemos comentado: las "PGP Tools", accesibles desde el icono de PGP, y que también permiten

cifrar,

borrar, etc., y que tienen el aspecto de la figura:

borrado de

El botón situado más a la derecha es el que permite el espacio libre, que elimina todos los restos de ficheros directorios, finales de ficheros, etc, etc...

borrados,

Convertirse en

usuario avanzado

comprobado

privacidad.

PGP es un programa muy completo y -como habrá

en este breve tutorial- una herramienta imprescindible para usuarios conscientes de Internet, preocupados por su

uso,

en la

El precio de tanta potencia es una relativa complejidad de

basada más en la dificultad de los conceptos a manejar, que

propia operativa del programa (muy similar a cualquier otra utilidad de las que habitualmente manejamos).

tintero

le

aquí su

hemos

muchos

adicionales

Lógicamente, un tutorial de una hora obliga a dejar en el

algunos conceptos importantes, opciones menos utilizadas y mecanismos algo más complejos. Por ello, desde Kriptópolis

aconsejamos encarecidamente que no considere finalizado

aprendizaje de PGP. Aunque podemos asegurarle que aquí

cubierto el 90% del uso habitual del programa, quedan

temas interesantes por explorar, algunas precauciones

que tomar y algunos riesgos que conviene conocer.

Afortunadamente (y con independencia de otros recursos disponibles en la Red), disponemos en la Red del manual completo de PGP traducido al español, donde se cubren de forma exhaustiva muchos de los temas que aquí no hemos tocado. Aconsejamos su lectura a cualquier usuario de PGP. también hay muchos documentos interesantes en nuestra sección de publicaciones.

una lista
han

No olvide tampoco que Kriptópolis pone a su disposición de correo con más de 750 usuarios, muchos de los cuales se encontrado idénticas dificultades que usted y están además deseosos de ayudarle.

Buena suerte y feliz correo seguro con PGP.

José Manuel Gómez
Editor de Kriptópolis
Julio de 2000