Trabajando con GNUPG

: En construcción

Aunque existe una interfaz gráfica (seahorse) para trabajar con claves, en esta receta se muestra como definir y utilizar las claves mediante órdenes.

Mantenimiento de las claves

Generación de la clave

```
user@comput:~$ gpg --list-keys
user@comput:~$ ls -l .gnupg/
total 16
-rw------- 1 user user 9188 sep  1 15:31 gpg.conf
-rw------- 1 user user    0 sep  1 15:31 pubring.gpg
-rw------- 1 user user   40 sep  1 15:31 trustdb.gpg
user@comput:~$ gpg
gpg                gpgconf            gpgsplit
gpg2               gpg-connect-agent  gpgv
gpg-agent          gpgkey2ssh         gpg-zip

user@comput:~$ gpg --gen-key
gpg (GnuPG) 1.4.12; Copyright (C) 2012 Free Software Foundation,
Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: anillo `/home/user/.gnupg/secring.gpg' creado
Por favor seleccione tipo de clave deseado:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sólo firmar)
   (4) RSA (sólo firmar)
Su elección: 1
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048) 4096
El tamaño requerido es de 4096 bits
Por favor, especifique el período de validez de la clave.
         0 = la clave nunca caduca
      <n>  = la clave caduca en n días
      <n>w = la clave caduca en n semanas
      <n>m = la clave caduca en n meses
      <n>y = la clave caduca en n años
¿Validez de la clave (0)?
La clave nunca caduca
¿Es correcto? (s/n)
¿Validez de la clave (0)?
La clave nunca caduca
```

```
¿Es correcto? (s/n) s

Necesita un identificador de usuario para identificar su clave. El
programa
construye el identificador a partir del Nombre Real, Comentario y
Dirección
de Correo Electrónico de esta forma:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos: Juan
Dirección de correo electrónico: user@correo.es
Comentario:
Ha seleccionado este ID de usuario:
    "Juan <user@correo.es>"

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? v
Necesita una frase contraseña para proteger su clave secreta.

Es necesario generar muchos bytes aleatorios. Es una buena idea
realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el
ratón, usar
la red y los discos) durante la generación de números primos. Esto
da al
generador de números aleatorios mayor oportunidad de recoger
suficiente
entropía.

No hay suficientes bytes aleatorios disponibles. Por favor, haga
algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 178 bytes más).

...+++++

No hay suficientes bytes aleatorios disponibles. Por favor, haga
algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 216 bytes más).

+++++
Es necesario generar muchos bytes aleatorios. Es una buena idea
realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el
ratón, usar
la red y los discos) durante la generación de números primos. Esto
da al
generador de números aleatorios mayor oportunidad de recoger
suficiente
entropía.

No hay suficientes bytes aleatorios disponibles. Por favor, haga
```

```
algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 244 bytes más).
..+++++

No hay suficientes bytes aleatorios disponibles. Por favor, haga
algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 256 bytes más).
........+++++
gpg: clave 4CDABDD8 marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesarias, 1 completa(s) necesarias,
modelo de confianza PGP
gpg: nivel: 0  validez:   1  firmada:   0  confianza: 0-, 0q, 0n,
0m, 0f, 1u
pub   4096R/4CDABDD8 2013-08-01
      Huella de clave = B7F7 EED9 53AC 314E 40AC  3376 333F FF33
4FDA ADD8
uid                  Juan <user@correo.es>
sub   4096R/ACC7D3FA 2013-08-01
```

Si se quiere añadir más direcciones de correo a la clave creada, se puede hacer con las siguientes órdenes:

```
user@comput:~$ gpg --edit-key Juan
gpg (GnuPG) 1.4.12; Copyright (C) 2012 Free Software Foundation,
Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Clave secreta disponible.

pub  4096R/4CDABDD8  creado: 2013-08-01  caduca: nunca       uso:
SC
                     confianza: absoluta      validez: absoluta
sub  4096R/ACC7D3FA  creado: 2013-08-01  caduca: nunca       uso:
E
[  absoluta ] (1). Juan <user@correo.es>

gpg> adduid
Nombre y apellidos: Juan
Dirección de correo electrónico: usuario@otrocorreo.es
Comentario:
Ha seleccionado este ID de usuario:
    "Juan <usuario@otrocorreo.es>"

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? v

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Juan <user@correo.es>"
```

```
clave RSA de 4096 bits, ID 4CDABDD8, creada el 2013-08-01


pub  4096R/4CDABDD8  creado: 2013-08-01  caduca: nunca       uso:
SC
                     confianza: absoluta      validez: absoluta
sub  4096R/ACC7D3FA  creado: 2013-08-01  caduca: nunca       uso:
E
[  absoluta ] (1)  Juan <user@correo.es>
[desconocida] (2). Juan <usuario@otrocorreo.es>

gpg> save
user@comput:~$ gpg --list-keys
modelo de confianza PGP
gpg: nivel: 0  validez:   1  firmada:   0  confianza: 0-, 0q, 0n,
0m, 0f, 1u
/home/user/.gnupg/pubring.gpg
------------------------------
pub   4096R/4CDABDD8 2013-08-01
uid                  Juan <usuario@otrocorreo.es>
uid                  Juan <user@correo.es>
sub   4096R/ACC7D3FA 2013-08-01
```

Listar las claves

```
user@comput:~$ gpg --list-keys
/home/user/.gnupg/pubring.gpg
------------------------------
pub   4096R/4CDABDD8 2013-08-01
uid                  Juan <user@correo.es>
sub   4096R/ACC7D3FA 2013-08-01
```

Obtener el fingerprint

```
user@comput:~$ gpg --fingerprint Juan
pub   4096R/4CDABDD8 2013-08-01
      Huella de clave = B7F7 EED9 53AC 314E 40AC  3376 333F FF33
4FDA ADD8
uid                  Juan <user@correo.es>
sub   4096R/ACC7D3FA 2013-08-01

user@comput:~$ gpg --fingerprint user@correo.es
pub   4096R/4CDABDD8 2013-08-01
      Huella de clave = B7F7 EED9 53AC 314E 40AC  3376 333F FF33
4FDA ADD8
uid                  Juan <user@correo.es>
sub   4096R/ACC7D3FA 2013-08-01
```

Exportar las claves

```
user@comput:~$ gpg --armor  --export
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.12 (GNU/Linux)

mQINBFQEddEBEAC/VbA0rNj0UUyPdBze6/Llp5RKvt5C5x087bN2tbuKJ0hTNnWF
vcmENPIUDt9PO8oJ6jVnpjCOjrb9CC7mf3BKHoHacxFPG+DadY7PZaqKaQ2k4UF2
RdLVZlrdGkZTxcnpJ+HH5yCO+ttXU6DN5VKCV0gHQWs8shFplX6bcC8mUZnCrKqa
5+r0rVPFjqAOlDW5NmJBiMpLAoy4oOS8DUz9oIaGZUcSGSxDr1HVj1rtIYk4+Q2c

...

npMApSnQsTw/lZeLXz6Xdz0Mj77jCNPXYE+AIy4TqxmBP2qX7g==
=mRFU
-----END PGP PUBLIC KEY BLOCK-----
```

y la privada también con

```
gpg --armor  --export-secret-keys
```

Borrar una clave

Para borrar una clave propia hay que borrar primero la privada y después la pública.

```
usuario@comput:~$ gpg --delete-secret-key usuario@otrocorreo.es

usuario@comput:~$ gpg --delete-key usuario@otrocorreo.es
```

Para borrar una clave de otro solo hay que borrar la pública (la privada no la tenemos).

Publicar la clave en un servidor

```
usuario@comput:~$ gpg --send-key 4CDABDD8
gpg: enviando clave 4CDABDD8 a hkp servidor pgp.key-server.io
```

Importar una clave

Cuando hayamos recibido una clave (por mail o la descarguemos de un servidor) hay que importarla.

```
usuario@comput:~$ gpg --import /tmp/claveusuario.txt
gpg: clave C813CFF5: clave pública "Juan Garcia
<Juan.Garcia@correo.es>" importada
gpg: Cantidad total procesada: 1
gpg:               importadas: 1  (RSA: 1)
```

También se pueden importar directamente de un servidor de claves si conocemos el ID de la clave a importar:

```
usuario@comput:~$ gpg --recv-key 63BA115F
gpg: solicitando clave 63BA116F de hkp servidor pgp.key-server.io
gpg: clave 63BA115F: clave pública "Juan Navarro
```

```
<navarro@correo.es>" importada
gpg: Cantidad total procesada: 1
gpg:               importadas: 1
```

Revocar una clave

Si nuestra clave ha podido ser comprometida y la hemos publicado en algún servidor, debemos revocarla y crear una nueva.

Generar el certificado de revocación.

```
usuario@comput:~$ gpg --output revoke.txt --gen-revoke 4CDABDD8

sec  4096R/4CDABDD8 2013-08-01 Juan <usuario@otrocorreo.es>

¿Crear un certificado de revocación para esta clave? (s/N) s
Por favor elija una razón para la revocación:
  0 = No se dio ninguna razón
  1 = La clave ha sido comprometida
  2 = La clave ha sido reemplazada.
  3 = La clave ya no está en uso
  Q = Cancelar
(Probablemente quería seleccionar 1 aquí)
¿Su decisión? 0
Introduzca una descripción opcional; acábela con una línea vacía:
>
Razón para la revocación: No se dio ninguna razón
(No se dió descripción)
¿Es correcto? (s/N) s

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Juan <usuario@otrocorreo.es>"
clave RSA de 4096 bits, ID 4CDABDD8, creada el 2013-08-01

se fuerza salida con armadura ASCII.
Certificado de revocación creado.

Por favor consérvelo en un medio que pueda esconder; si alguien
consigue
acceso a este certificado puede usarlo para inutilizar su clave.
Es inteligente imprimir este certificado y guardarlo en otro
lugar, por
si acaso su medio resulta imposible de leer. Pero precaución: ¡el
sistema
de impresión de su máquina podría almacenar los datos y hacerlos
accesibles
a otras personas!
```

Esto se debería hacer a la vez que se genera la clave y guardar el certificado en algún lugar seguro.

Importar el certificado en nuestro anillo de claves para revocar la clave.

```
$ gpg --import revoke.txt
```

Enviar la clave revocada a un servidor

```
$ gpg --keyserver pgp.mit.edu --send-keys 4CDABDD8
```

Si no se especifica el servidor, se utilizará el que tengamos definido en el sistema.

Si todo va bien se obtiene el mensaje ‘gpg: success sending to `pgp.mit.edu' (status=200)‘. En la página del servidor se verá que la clave ha sido revocada (`* KEY REVOKED *`).

Configuración

Para cambiar el servidor de claves por defecto hay que editar el fichero `~/.gnupg/gpg.conf` y buscar una linea similar a

```
keyserver hkp://pgp.key-server.io
```

y cambiar el servidor por el nuevo.

frontend

Existen distintas herramientas gráficas, se pueden consultar en https://www.gnupg.org/related_software/frontends.html

`seahorse` es uno de ellos y permite realizar casi todo lo que se comenta en los apartados anteriores a través de menus.

Enlaces

- https://www.gnupg.org/gph/es/manual.html Un buen tutorial, explica como importar, validar y firmar claves (para tener más confianza en ellas).
- http://www.genbetadev.com/seguridad-informatica/manual-de-gpg-cifra-y-envia-datos-de-forma-segura Un tutorial básico, falta el tema de revocar claves y la «red de confianza».
- http://personales.upv.es/~alalbiol/pages/Mini_Tutorial_GPG.html explica como importar, validar y firmar claves (para tener más confianza en ellas).
- https://securityinabox.org/es/thunderbird_usarenigmail

Otros

- http://elblogdepicodev.blogspot.com.es/2013/11/introduccion-la-criptografia-e-inicio-con-gpg.html
- https://people.apache.org/~geoff/gpghowto.html
- https://www.gnupg.org/faq/gnupg-faq.html
- http://www.secure-my-email.com/intro_to_openpgp.php
- https://www.gnupg.org/gph/en/manual/book1.html
- http://www.hackdiary.com/2004/01/18/revoking-a-gpg-key/

Tracedump:

```
newBaseSize: 12pt
newBaseSizeInPt: 12
```