# Firmas digitales con GnuPG


## Alberto Pesquera Martín

## Manuel A. Fernández Montecelo


## 1. Introducción

> **Nota:** Este apartado esta en construcción. Debido a la posible extensión que se le podría dar al tema, junto con toda su reflexión.

Adjunto un guión de lo que me gustaría que rellenase este hueco:

Firmas
Firmas Digitales
PGP y GnuPG
Validez legal

## 2. Generación de nuestra clave

### 2.1. Paso a paso

Pues nos ponemos a ello:

```
$ gpg --gen-key

  gpg (GnuPG) 1.2.0; Copyright (C) 2002 Free Software Foundation, Inc.
  This program comes with ABSOLUTELY NO WARRANTY.
  This is free software, and you are welcome to redistribute it
  under certain conditions. See the file COPYING for details.

  gpg: keyring ‘/home/apmso/.gnupg/secring.gpg’ created
  Please select what kind of key you want:
  (1) DSA and ElGamal (default)
  (2) DSA (sign only)
  (5) RSA (sign only)
  Your selection? 1
  DSA keypair will have 1024 bits.
  About to generate a new ELG-E keypair.
              minimum keysize is  768 bits
              default keysize is 1024 bits
      highest suggested keysize is 2048 bits
  What keysize do you want? (1024)
```

```
Requested keysize is 1024 bits
Please specify how long the key should be valid.
     0 = key does not expire
  <n>  = key expires in n days
  <n>w = key expires in n weeks
  <n>m = key expires in n months
  <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct (y/n)? y

You need a User-ID to identify your key; the software constructs the user id
from Real Name, Comment and Email Address in this form:
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Alberto Pesquera Martín
Email address: apm@sindominio.net
Comment:
You selected this USER-ID:
"Alberto Pesquera Martín <apm@sindominio.net>"

  Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.

Enter passphrase:
Repeat passphrase:

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.

/home/apm/.gnupg/trustdb.gpg: trustdb created
fpublic and secret key created and signed.
key marked as ultimately trusted.

pub  1024D/6DA790AC 2002-12-12 Alberto Pesquera Martín <apm@sindominio.net>
Key fingerprint = 0846 8248 DEE5 7E7C FAA7  91B0 AD99 E8DA 6DA7 90AC
sub  1024g/EDB53196 2002-12-12
```

Con esto ya tenemos una clave gpg para firmar nuestros mensajes de correo electrónico.

## 2.2. Exportar la clave pública

Para que puedan saber que somos nosotros los que firmamos el mensaje, debemos darles nuestra clave pública. Que es sólamente una parte de nuestro sistema de *Firma Digital*, de cara a los demas.

Para ello exportamos nuestra clave: `gpg --export -a <usuario>`

```
$ gpg --export -a apm > clave-pub.asc
```

> **Nota:** La opción *-a* sirve para exportar la clave en formato ascii (*texto*).
>
> Y la opción > redirecciona la salida a un archivo (`clave-pub.asc`); ya que sino la clave pública simplemente aparecería en la pantalla.

Ahora solo queda ponerla disponible al público, bien mediante la página web personal, un anillo de claves, o un servidor de claves.

> **Nota:** Se recomienda NO adjuntar la clave pública en los mensajes de correo electrónico, ya que SÓLO genera *ruido*. A cambio se suele poner un enlace a la misma, y/o la huella dactilar (fingerprint).

# 3. Identidades

Las identidades sirven para utilizar una misma clave con varias cuentas de correo electrónico, sin tener que generar varias claves para cada una de esas cuentas de correo electrónico.

## 3.1. Generación de nuevas identidades

Para ello ejecutamos: gpg --edit-key <usuario>

```
$ gpg --edit-key apm
Orden> adduid

Nombre y Apellidos: Alberto Pesquera Martín
Dirección de correo electrónico: apm@ii.uned.es
Comentario:
Está usando el juego de caracteres ‘iso-8859-1’.
Ha seleccionado este ID de usuario:
"Alberto Pesquera Martín <apm@ii.uned.es>"

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

       Necesita una contraseña para desbloquear la clave secreta
del usuario: "Alberto Pesquera Martín <apm@sindominio.net>"
clave DSA de 1024 bits, ID 6DA790AC, creada el 2002-12-12

Introduzca contraseña:
```

```
pub  1024D/6DA790AC  creada: 2002-12-12 expira: never      confianza: u/u
sub  1024g/EDB53196  creada: 2002-12-12 expira: never
(1)  Alberto Pesquera Martín <apesquera@bec.uned.es>
(2)  Alberto Pesquera Martín <apm@sindominio.net>
(3). Alberto Pesquera Martín <apm@ii.uned.es>

Orden> save
```

Ya esta creada las identidades de las cuentas de correo electrónico anteriores con una sola firma GPG.

## 3.2. Selección de la Identidad Primaria

Cuando añadimos mas identidades a una firma digital, esta última identidad añadida es la GnuPGque toma como primaria. Si queremos cambiar la identidad primaria, editamos la clave: `gpg --edit-key <usuario>`

```
$ gpg --edit-key apm

  gpg (GnuPG) 1.2.0; Copyright (C) 2002 Free Software Foundation, Inc.
  This program comes with ABSOLUTELY NO WARRANTY.
  This is free software, and you are welcome to redistribute it
  under certain conditions. See the file COPYING for details.

  Clave secreta disponible.

  pub  1024D/6DA790AC  creada: 2002-12-12 expira: never      confianza: u/u
  sub  1024g/EDB53196  creada: 2002-12-12 expira: never
  (1)  Alberto Pesquera Martín <apesquera@bec.uned.es>
  (2)  Alberto Pesquera Martín <apm@sindominio.net>
  (3). Alberto Pesquera Martín <apm@ii.uned.es>
```

Seleccionamos la identidad que queremos que sea la primaria

```
Orden> uid 2

  pub  1024D/6DA790AC  creada: 2002-12-12 expira: never      confianza: u/u
  sub  1024g/EDB53196  creada: 2002-12-12 expira: never
  (1)  Alberto Pesquera Martín <apesquera@bec.uned.es>
  (2)* Alberto Pesquera Martín <apm@sindominio.net>
  (3). Alberto Pesquera Martín <apm@ii.uned.es>
```

E indicamos que esa identidad es la primaria.

```
Orden> primary

  Necesita una contraseña para desbloquear la clave secreta
  del usuario: "Alberto Pesquera Martínn <apm@ii.uned.es>"
  clave DSA de 1024 bits, ID 6DA790AC, creada el 2002-12-12


  pub  1024D/6DA790AC  creada: 2002-12-12 expira: never      confianza: u/u
  sub  1024g/EDB53196  creada: 2002-12-12 expira: never
  (1)  Alberto Pesquera Martín <apesquera@bec.un
  (2)* Alberto Pesquera Martín <apm@sindominio.net>
  (3)  Alberto Pesquera Martín <apm@ii.uned.es>

Orden> save
```

# 4. Proceso de Firmas

> **Nota:** Me hubiera gustado rellenar esta sección con los ejemplos tan completos como las anteriores. Espero hacerlo en unos pocos días. Ya que este proceso no es únicamente la importación de la clave de la otra persona.

Consiste en verificar que la firma incluida en el mensaje de correo electrónico pertenece a la persona quien dice ser. Para validar la autentificación de la firma. Se realiza el proceso llamado *Firma de claves*.

En este proceso se recomienda seguir el protocolo de verificación de identidad descrito en profundidad en http://www.gnupg.org/gph/en/manual/book1.html que aquí se tratará por encima. Ya que el proposito del protocolo es la completa verificación de la identidad de la/s persona/s.

Obtenemos la clave pública de la otra persona. Y la importamos a la base de datos de gpg.

```
$ gpg --import -a clave-pub-.asc
```

Ahora la editamos, comprobamos la huella dactilar (fingerprint) y, si está todo correcto, la firmamos:

```
$ gpg --edit-key manuel
Orden> sign
Orden> save
```

Una vez firmada, exportamos la clave firmada de la otra persona; con esto la otra persona puede comprobar que hemos firmado su clave. Y cuando ella exporte su clave, otros podrán comprobar que tu has firmado su clave, pudiendose asi establecer *relaciones de confianza*.

```
$ gpg --export -a manuel > manuel-SD.asc
```

Y cuando la otra persona nos devuelva nuestra clave firmada, importamos esta para actualizar la base de datos de gpg:

```
$ gpg --import -a apm-SD.asc
```

Si queremos comprobar quien nos ha firmado la clave:

```
$ gpg --list-sigs apm
```

```
pub  1024D/6DA790AC 2002-12-12 Alberto Pesquera Martín <apm@sindominio.net>
sig 3       6DA790AC 2002-12-13   Alberto Pesquera Martín <apm@sindominio.net>
sig         6B6048E5 2002-12-16   Miguel Angel Cordova Morales (Tec-InFor - Desarrollo Tecnologico de
uid                           Alberto Pesquera Martín <apesquera@bec.uned.es>
sig 3       6DA790AC 2002-12-12   Alberto Pesquera Martín <apm@sindominio.net>
sig 3       93FBC761 2002-12-13   Manuel A. Fernández Montecelo <manuel@sindominio.net>
sig         6B6048E5 2002-12-16   Miguel Angel Cordova Morales (Tec-InFor - Desarrollo Tecnologico de
uid                           Alberto Pesquera Martín <apm@ii.uned.es>
sig 3       6DA790AC 2002-12-16   Alberto Pesquera Martín <apm@sindominio.net>
sig         6B6048E5 2002-12-16   Miguel Angel Cordova Morales (Tec-InFor - Desarrollo Tecnologico de
sub  1024g/EDB53196 2002-12-12
sig         6DA790AC 2002-12-12   Alberto Pesquera Martín <apm@sindominio.net>
```