

Grado en Ingeniería Informática
Seguridad en Tecnologías de la Información
Curso 2017/18

Práctica Número 2



UNIVERSIDAD DE JAÉN

Autor: Manuel Alférez Ruiz

Generación de clave pública/privada

En esta práctica vamos a crear una *clave pública* y otra *privada*. Una vez ya este creada siguiendo el manual de la práctica procedemos a verificar que las claves se han creado correctamente y que su plazo de validez es de hasta 10 meses:

```
$ gpg --list-keys
```

Escribiendo este comando en la terminal obtendremos por pantalla nuestras claves:

La salida sería la siguiente:

```
pub 4096R/7A5CA982 2017-09-28 [[caduca: 2018-07-25]]
uid          Manuel Alferez Ruiz (Manuel)
sub 4096R/BFCB6BE1 2017-09-28 [[caduca: 2018-07-25]]
```

Esta imagen nos proporciona mucha información, como puede ser:

- El identificador de la clave generada: 7A5CA982
- La fecha en el que fue creada: 2017-09-28
- La fecha en la que caducará nuestra clave: 2018-07-25
- El nombre a quien está asociada: Manuel Alferez Ruiz
- Su correo electrónico: [REDACTED]

Exportación de la clave pública

A continuación, escribiendo en la terminal:

```
~/Escritorio $ gpg -a --export Manuel > 7A5CA982_pub.asc
```

Podremos con esta acción exportar nuestra clave pública en un fichero llamado *7A5CA982_pub* con formato *.asc*. En dicho fichero tenemos almacenada nuestra clave pública en *formato ASCII*, que como sabemos resulta interesante para proporcionar a otras personas nuestra clave pública.



Firma de mensaje

A continuación vamos a crear un archivo *.txt* para almacenar información en su interior. Y vamos a firmar digitalmente el archivo:

```
$ gpg --clearsign mensaje.txt
```

Con este comando queda firmado nuestro mensaje. Nos debería de mostrar este mensaje por la terminal después de introducir la clave:

```
Necesita una contraseña para desbloquear la clave secreta
del usuario: "Manuel Alferez Ruiz (Manuel)"
clave RSA de 4096 bits, ID 7A5CA982, creada el 2017-09-28
```

keyserver.ubuntu.com

SKS OpenPGP Public Key Server

Extracting a OpenPGP Key

Index: ● Verbose Index: ●

Search String:

☒ Show OpenPGP "fingerprints" for keys

☐ Only return exact matches

Submitting a new OpenPGP Key

Enter ASCII-armored OpenPGP key here:

keyserver.ubuntu.com/pks/lookup?op=vindex&search=Manuel+Alferez&fingerprint=on

Search results for 'manuel alferez'

| Type | bits/keyID | cr. time | exp time | key expir |
|------|--|------------|------------|---------------------------|
| pub | 4096R/7A5CA982 | 2017-09-28 | | |
| uid | Manuel Alferez Ruiz (Manuel) <mar00049@red.ujaen.es> | | | |
| sig | sig3 7A5CA982 | 2017-09-28 | 2018-07-25 | [selfsig] |
| sub | 4096R/BFCB6BE1 | 2017-09-28 | | |
| sig | sig sbind 7A5CA982 | 2017-09-28 | 2018-07-25 | [i] |

Como podemos ver en las imágenes, la clave pública ha sido subida con éxito.

4

Esta acción nos genera un archivo con terminación *.asc* que sería nuestro mensaje ya firmado con la firma digital:



Contenido de *mensaje.txt.asc*:

```
mensaje.txt.asc
~Escritorio

Archivo  Editar  Ver  Buscar  Herramientas  Documentos  Ayuda

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Nombre: Manuel Alferéz Ruiz
DNI: [REDACTED]
Grupo (Teoría): A
Grupo (Prácticas): 4
Curso académico: Segundo
Huella de clave = 1F2B B426 06B5 F1ED 466A 2430 1CF9 AE4A 7A5C A982
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

[REDACTED]

=wJtL
-----END PGP SIGNATURE-----

Texto plano  Anchura de la pestaña: 8  Ln 1, Col 1  INS
```

Subiendo la clave pública a un servidor de claves

A continuación procedemos a enviar nuestra clave pública a un servidor de claves:

```
administrador@administrador-Lenovo-Z50-70 ~/Escritorio $ gpg --keyserver hkp://keyserver.ubuntu.com:80 --send-keys 7A5CA982
gpg: enviando clave 7A5CA982 a hkp servidor keyserver.ubuntu.com
```

Ya se ha quedado enviada mi clave al servidor *keyserver.ubuntu.com*. Corrobores de que la subida se ha realizado con éxito buscando en el servidor: