

# Git en un servidor - Generando tu clave pública SSH

## Generando tu clave pública SSH

Tal y como se ha comentado, muchos servidores Git utilizan la autenticación a través de claves públicas SSH. Y, para ello, cada usuario del sistema ha de generarse una, si es que no la tiene ya. El proceso para hacerlo es similar en casi cualquier sistema operativo. Ante todo, asegurarte que no tengas ya una clave. Por defecto, las claves de cualquier usuario SSH se guardan en la carpeta `~/.ssh` de dicho usuario. Puedes verificar si tienes ya unas claves, simplemente situándote sobre dicha carpeta y viendo su contenido:

```
$ cd ~/.ssh
$ ls
authorized_keys2  id_dsa          known_hosts
config           id_dsa.pub
```

Has de buscar un par de archivos con nombres tales como 'algo' y 'algo.pub'; siendo ese "algo" normalmente 'idrsa' o 'idrsa'. El archivo terminado en '.pub' es tu clave pública, y el otro archivo es tu clave privada. Si no tienes esos archivos (o no tienes ni siquiera la carpeta '.ssh'), has de crearlos; utilizando un programa llamado 'ssh-keygen', que viene incluido en el paquete SSH de los sistemas Linux/Mac o en el paquete MSysGit en los sistemas Windows:

```
$ ssh-keygen

Generating public/private rsa key pair.

Enter file in which to save the key (/Users/schacon/.ssh/id_rsa):

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /Users/schacon/.ssh/id_rsa.
Your public key has been saved in /Users/schacon/.ssh/id_rsa.pub.

The key fingerprint is:
43:c5:5b:5f:b1:f1:50:43:ad:20:a6:92:6a:1f:9a:3a
schacon@agadorlaptop.local
```

Como se vé, este comando primero solicita confirmación de dónde van a guardarse las claves ('.ssh/id\_rsa'), y luego solicita, dos veces, una contraseña (passphrase), contraseña que puedes dejar en blanco si no deseas tener que teclearla cada vez que uses la clave.

Tras generarla, cada usuario ha de encargarse de enviar su clave pública a quienquiera que administre el servidor Git (en el caso de que este esté configurado con SSH y así lo requiera). Esto se puede realizar simplemente copiando los contenidos del archivo terminado en '.pub' y enviándoselos por correo electrónico. La clave pública será una serie de números, letras y signos, algo así como esto:

```
$ cat ~/.ssh/id_rsa.pub  
ssh-rsa  
AAAAB3NzaC1yc2EAAAABIwAAAQEAKlOUpkDHrfHY17SbrmTIpNLTKG9Tjom/BWDSU  
GPl+nafz1HDTYW7hdI4yZ5ew18JH4JW9jbhUFrviQzM7xlELEVf4h91FX5QVkbPppS  
wg0cda3Pbv7kOdJ/MTyBlWXFCR+HAo3FXRitBqxiX1nKhXpHAZsMciLq8V6RjsNAQw  
dsdMFvSlVK/7XAt3FaoJoAsncM1Q9x5+3V0Ww68/eIFmb1zuUFljQJKprX88XypND  
vjYNby6vw/Pb0rwert/EnmZ+AW4OZPnTPI89ZPmVMLuayrD2cE86Z/il8b+gw3r3+1  
nKatmIkjn2sold0lQraTlMqVSsbxNrRFi9wrf+M7Q==  
schacon@agadorlaptop.local
```