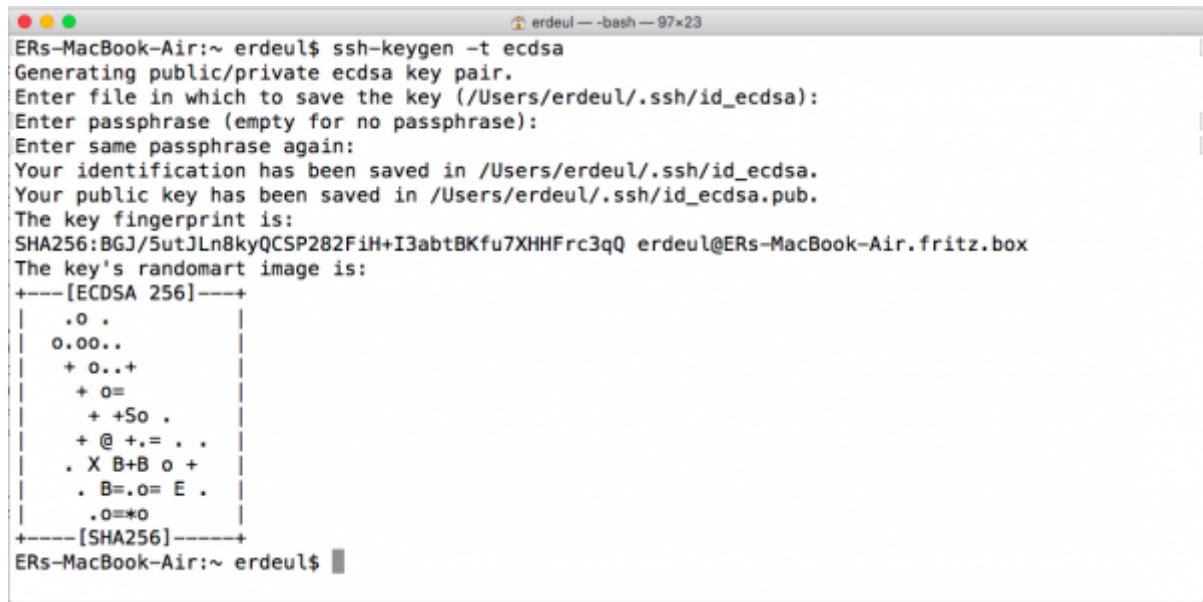


Setup key based login from MacOS

The procedure is very similar to the Linux procedure. So we first need to build a public/private keypair using the ssh-keygen utility:



```

ERs-MacBook-Air:~ erdeul$ ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/Users/erdeul/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/erdeul/.ssh/id_ecdsa.
Your public key has been saved in /Users/erdeul/.ssh/id_ecdsa.pub.
The key fingerprint is:
SHA256:BGJ/5utJLn8kyQCSP282FiH+I3abtBKfu7XHHFrc3qQ erdeul@ERs-MacBook-Air.fritz.box
The key's randomart image is:
+----[ECDSA 256]-----+
|  .o .                  |
| 0.00..                 |
| + o..+                 |
| + o=                   |
| + +So .                |
| + @ +. = . .          |
| . X B+B o +           |
| . B=.o= E .           |
| .o=*o                 |
+----[SHA256]-----+
ERs-MacBook-Air:~ erdeul$

```

For both question about passphrase, just hit enter (we will not be using passphrases). This will also have generated two files in your personal .ssh directory:

```

elstar:Desktop administrator$ ls -l ~/.ssh/id*
-rw----- 1 administrator staff 1831 Jul 9 11:08 /Users/administrator/.ssh/id_rsa
-rw-r--r-- 1 administrator staff 408 Jul 9 11:08 /Users/administrator/.ssh/id_rsa.pub

```

The file id_rsa.pub must be transferred to the remote host. For this we can use ssh-copy-id:

```
$ ssh-copy-id -i ~/.ssh/id_ecdsa.pub username@remote-host
```

This may produce the following message:

```

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/home/username/.ssh/id_rsa.pub"
The authenticity of host 'remote-host (123.123.123.123)' can't be
established.
ECDSA key fingerprint is SHA256:tygMarTe3S0jTcY9HzldKThxQzsTeiYHg5JmjB2bxeg.
Are you sure you want to continue connecting (yes/no)? yes

```

Having confirmed the access key to remote-host, the copy operation will commence:

```

/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to
filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are
prompted now it is to install the new keys
username@remote-host's password:

```

Type your password to actually start the file copy.

Number of key(s) added: 1

Now try logging into the machine, with: `"ssh 'username@remote-host'"`
and check to make sure that only the key(s) you wanted were added.

The passwordless/2fa codeless ssh login is now in place.

From:

<https://helpdesk.strw.leidenuniv.nl/wiki/> - **Computer Documentation Wiki**

Permanent link:

<https://helpdesk.strw.leidenuniv.nl/wiki/doku.php?id=services:2fa:ssh:macos&rev=1616416759>

Last update: **2021/03/22 12:39**

