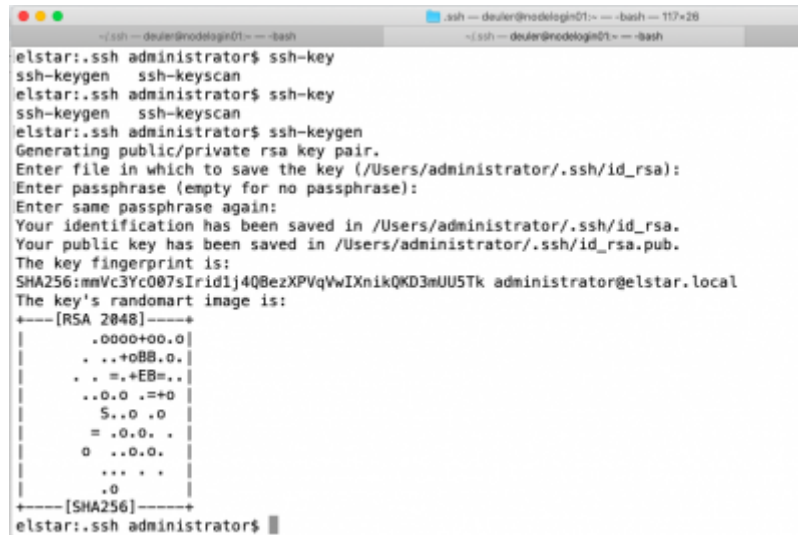


# Setup key based login from MacOS

The procedure is very similar to the Linux procedure. So we first need to build a public/private keypair using the ssh-keygen utility (note here the default rsa key is generated, but it is more secure to generate an ecdsa key like `ssh-keygen -t ecdsa`):



```

elstar:ssh administrator$ ssh-key
ssh-keygen  ssh-keyscan
elstar:ssh administrator$ ssh-key
ssh-keygen  ssh-keyscan
elstar:ssh administrator$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/administrator/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/administrator/.ssh/id_rsa.
Your public key has been saved in /Users/administrator/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:mmVc3Yc007sIrid1j4Q8ezXPVqVwIXnikQKD3mUU5Tk administrator@elstar.local
The key's randomart image is:
+--[RSA 2048]--++
|      .000+00.0 |
|      . ..+0BB.0. |
|      . .+.EB=. . |
|      ..0.0 .+=+0 |
|      S..0 .0      |
|      =.0.0. .     |
|      0 ..0.0.     |
|      +..+..+     |
|      .0          |
+-----[SHA256]-----+
elstar:ssh administrator$

```

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` (again the image shows the rsa keypair, but you better use a ecdsa key pair):

```
$ 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=1616413103>

Last update: **2021/03/22 11:38**

