**Configure user public key authentication to Pi Kodi**

Configuring public key authentication involves generating a key pair for a user, installing the public key on the remote host, and ensuring permissions and ovwnership of the key files are correct.

**o Verify that “publickey” authentication is possible to the SSH server:**$ **ssh -v 192.168.0.6**

OpenSSH\_6.8p1, OpenSSL 1.0.2a 19 Mar 2015

debug1: Connecting to 192.168.0.6 [192.168.0.6] port 22.

debug1: Connection established.

…

debug1: Authentications that can continue: **publickey**,password,keyboard-interactive

debug1: Next authentication method: password

jcdc@192.168.0.6's password:

**o Generate a client-side user key pair using the OpenSSH utility “ssh-keygen”.**  
**Note**: If you generate a new key pair, you will need to update your github account with the new client-side public key. See here <https://github.com/settings/keys>

$ **ssh-keygen -t rsa -b 1024**

Generating public/private rsa key pair.

Enter file in which to save the key (/home/jcdc/.ssh/id\_rsa):

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/jcdc/.ssh/id\_rsa.

Your public key has been saved in /home/jcdc/.ssh/id\_rsa.pub.

The key fingerprint is:

SHA256:hBeDRPYsbI3KQIzR3OW45jIruz+JkzRQff5ug8AXEYA jcdc@e1317t

The key's randomart image is:

+---[RSA 1024]----+

|.\*.+.=\*oo |

|..E o=+\* o |

| .. .oB.\* |

|. o +o+ |

|. .= oS |

| o oo . . |

|.o+..o o |

|= o+ . + |

|o\*o. . . |

+----[SHA256]-----+

jcdc@e1317t ~/.ssh

$ wpwd

C:\cygwin\home\jcdc\.ssh

jcdc@e1317t ~/.ssh

$ ls -altr

total 17

drwxr-xr-x+ 1 jcdc None 0 Feb 12 20:13 ..

-rw-r--r-- 1 jcdc None 225 Feb 13 18:09 **id\_rsa.pub**

-rw------- 1 jcdc None 887 Feb 13 18:09 **id\_rsa**

drwx------+ 1 jcdc None 0 Feb 13 18:09 .

jcdc@e1317t ~/.ssh

$ date

13 Feb 2018 18:09:31  
**Note:** I did not specify a passphrase for my private key. Although this is not recommended, it avoids me having to use an ssh-agent tool such as Keychain.  
  
  
**o Copy the client-side public key to the Pi.**The root user ~/.ssh directory on the Pi is initially empty:  
OpenELEC:~/.ssh # pwd

/storage/.ssh

OpenELEC:~/.ssh # ls -altr

total 2

drwx------ 2 root root 1024 Jan 1 1970 .

drwxr-xr-x 16 root root 1024 Feb 6 21:16 ..

On my Netbook we copy the client-side public key to the Pi “authorized\_keys” file:   
jcdc@e1317t ~/.ssh

$ wpwd

C:\cygwin\home\jcdc\.ssh

**scp id\_rsa.pub** [**root@192.168.0.6:/tmp**](mailto:root@192.168.0.6:/tmp)The authenticity of host '192.168.0.6 (192.168.0.6)' can't be established.

ECDSA key fingerprint is SHA256:bHvWnxk8UPVFP/ilWK32WNKOq/1oIsvQMcEy0WTveqI.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.0.6' (ECDSA) to the list of known hosts.

root@192.168.0.6's password:

**$ ssh -t root@192.168.0.6 "cat /tmp/id\_rsa.pub >> ~/.ssh/authorized\_keys"**

root@192.168.0.6's password:

Connection to 192.168.0.6 closed.

The root user ~/.ssh directory on the Pi now contains the following:  
OpenELEC:~/.ssh # pwd

/storage/.ssh

OpenELEC:~/.ssh # ls -altr

total 3

drwxr-xr-x 16 root root 1024 Feb 6 21:16 ..

-rw-r--r-- 1 root root 225 Feb 13 18:38 **authorized\_keys**

drwx------ 2 root root 1024 Feb 13 18:38 .  
OpenELEC:~/.ssh # cat authorized\_keys

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDAJmcssVTGgGlfrYa6PRhZmLVZIFYqJ0gyflvq8rk6PLtUK/4FHr7muD3jwwnWTEJ+HOQv67V5FeAXWT87JtWDWrAw8nEH7+BUm3lskY+tFiTL9SAbSFIgQ/h3vuXZA0wBPmFcCOEEVdlDXP9w3MuqhPwKQkJDRdazcFWncGTYbQ== **jcdc@e1317t**

Because we connected successfully to the Pi, we now have the public key of the Pi in the client-side “known\_hosts” file:  
$ wpwd

C:\cygwin\home\jcdc\.ssh

jcdc@e1317t ~/.ssh

$ ls -altr

total 18

drwxr-xr-x+ 1 jcdc None 0 Feb 12 20:13 ..

-rw-r--r-- 1 jcdc None 225 Feb 13 18:09 id\_rsa.pub

-rw------- 1 jcdc None 887 Feb 13 18:09 id\_rsa

-rw-r--r-- 1 jcdc None 173 Feb 13 18:28 **known\_hosts**

drwx------+ 1 jcdc None 0 Feb 13 18:42 .

jcdc@e1317t ~/.ssh

$ cat known\_hosts

**192.168.0.6** ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGmgNigtxONtPQiVEhYGbaF9xkeKiL2ElWK66ezLTk1YD0p+pwCyS1NCz0ZkZ6VSHgvYw3eIjVb9p9Vpe4faMt4=

**o Ensure the permissions of the .ssh directory and files are as restrictive as possible.**Owner-controlled directoeis are best (700), but 750 permissions will still allow public key authentication to work:  
  
OpenELEC:~ # pwd

/storage

OpenELEC:~ # **chmod 700 .ssh**

OpenELEC:~ # ls -ld .ssh

**drwx------ 2 root root 1024 Feb 13 18:38 .ssh**  
OpenELEC:~/.ssh # **chmod 600 authorized\_keys**

OpenELEC:~/.ssh # ls -altr

total 3

drwxr-xr-x 16 root root 1024 Feb 6 21:16 ..

**-rw------- 1 root root 225 Feb 13 18:38 authorized\_keys**

drwx------ 2 root root 1024 Feb 13 18:38 .

**o Verify that the client can now access the Pi without being prompted for a password:**jcdc@e1317t ~/.ssh

$ **ssh -t root@192.168.0.6 "ls -altr"**

total 689

drwxr-xr-x 2 root root 1024 Jan 1 1970 videos

drwxr-xr-x 2 root root 1024 Jan 1 1970 tvshows

drwxr-xr-x 2 root root 1024 Jan 1 1970 pictures

drwxr-xr-x 2 root root 1024 Jan 1 1970 music

drwxr-xr-x 2 root root 1024 Jan 1 1970 .update

drwxr-xr-x 26 root root 1024 Jan 1 1970 .dvdcss

drwxrwxr-x 16 root root 226 Mar 1 2016 ..

drwx------ 2 root root 12288 Mar 1 2016 lost+found

drwxr-xr-x 2 root root 1024 Jan 1 2017 screenshots

drwxr-xr-x 2 root root 1024 Apr 17 2017 mywallpapers

-rw-r--r-- 1 root root 1663 Aug 5 2017 .swfinfo

----r-x--- 1 root root 228 Feb 4 13:08 MyRSSFeed.xml

drwxr-xr-x 11 root root 1024 Feb 6 21:03 .config

drwxr-xr-x 9 root root 1024 Feb 6 21:08 .cache

-rwxr-xr-x 1 root root 4607 Feb 6 21:16 genrssxml.py

-rw------- 1 root root 2759 Feb 6 21:16 .ash\_history

drwxr-xr-x 16 root root 1024 Feb 6 21:16 .

drwx------ 2 root root 1024 Feb 13 18:38 .ssh

-rw-r--r-- 1 root root 598 Feb 13 18:45 MyGeneratedRSSFeed.xml  
  
  
**All working 😊**

*JeremyC 13-02-2018***END**