

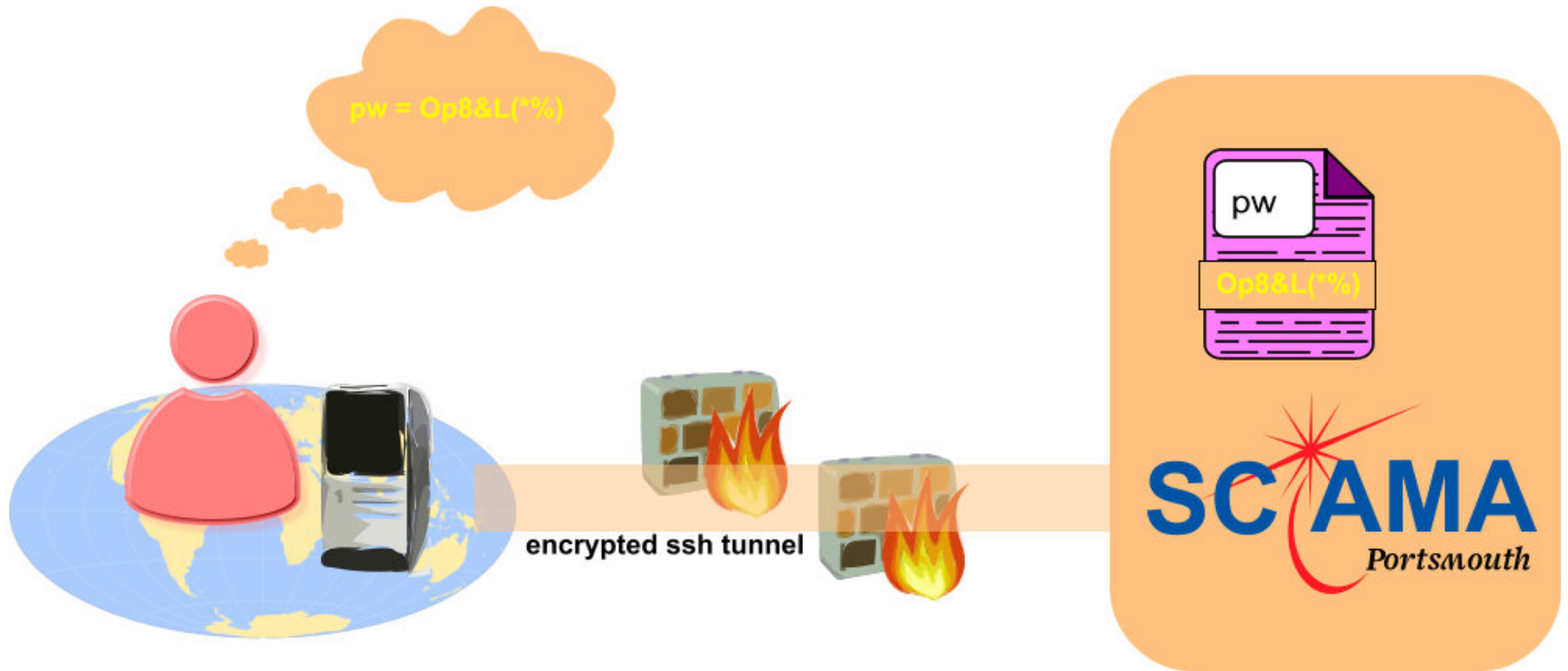


SSH Keys

G Burton – ICG – May18 – v1.1

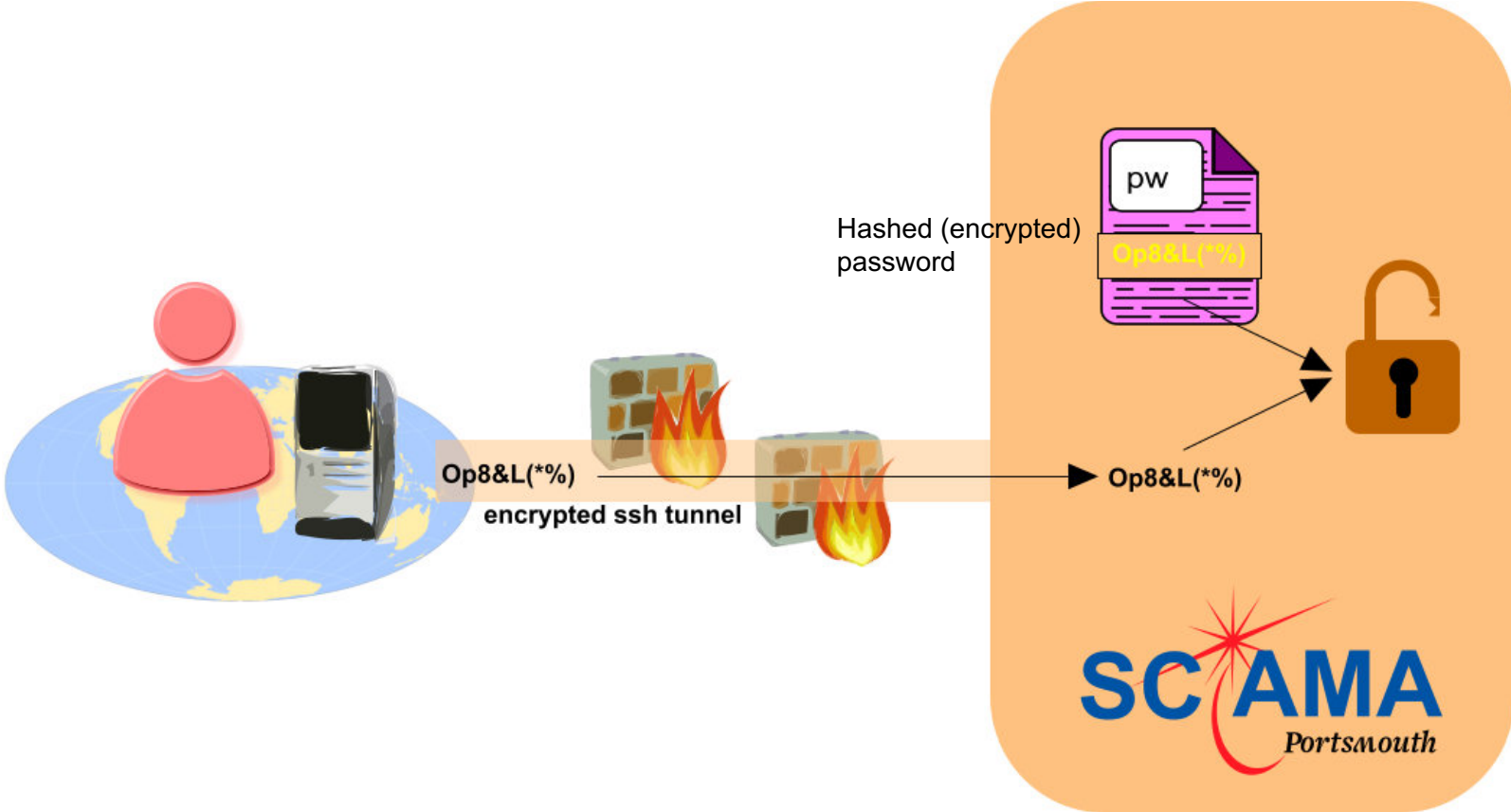


Passwords – What you know

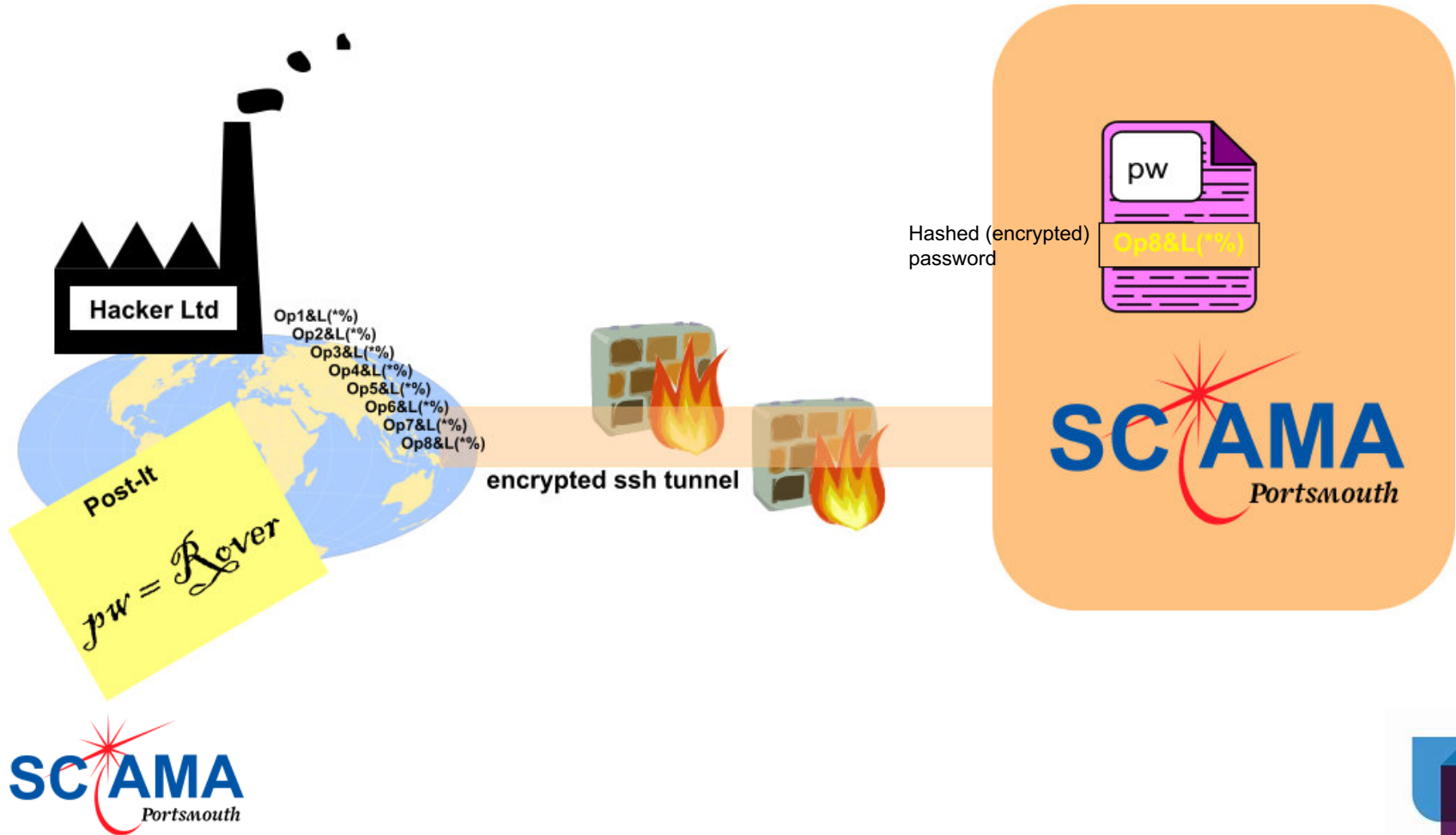


“yppasswd” can be used to change your password on Sciam.

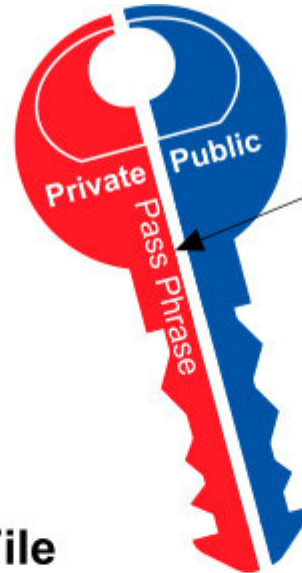
Encrypted pw compared with passwd file on Sciama



Brute force and ignorance



Introducing the SSH Key (pair)



Pass Phrase

Associated with the key is a Pass Phrase. It is mandatory to use a Pass Phrase.

Private Key File

Stored on your desktop or laptop

The pass phrase protects the private key



Public Key File

Stored on Sciama in \$HOME/.ssh/authorized_keys



Gobbledygook (eg. Ssh key file)

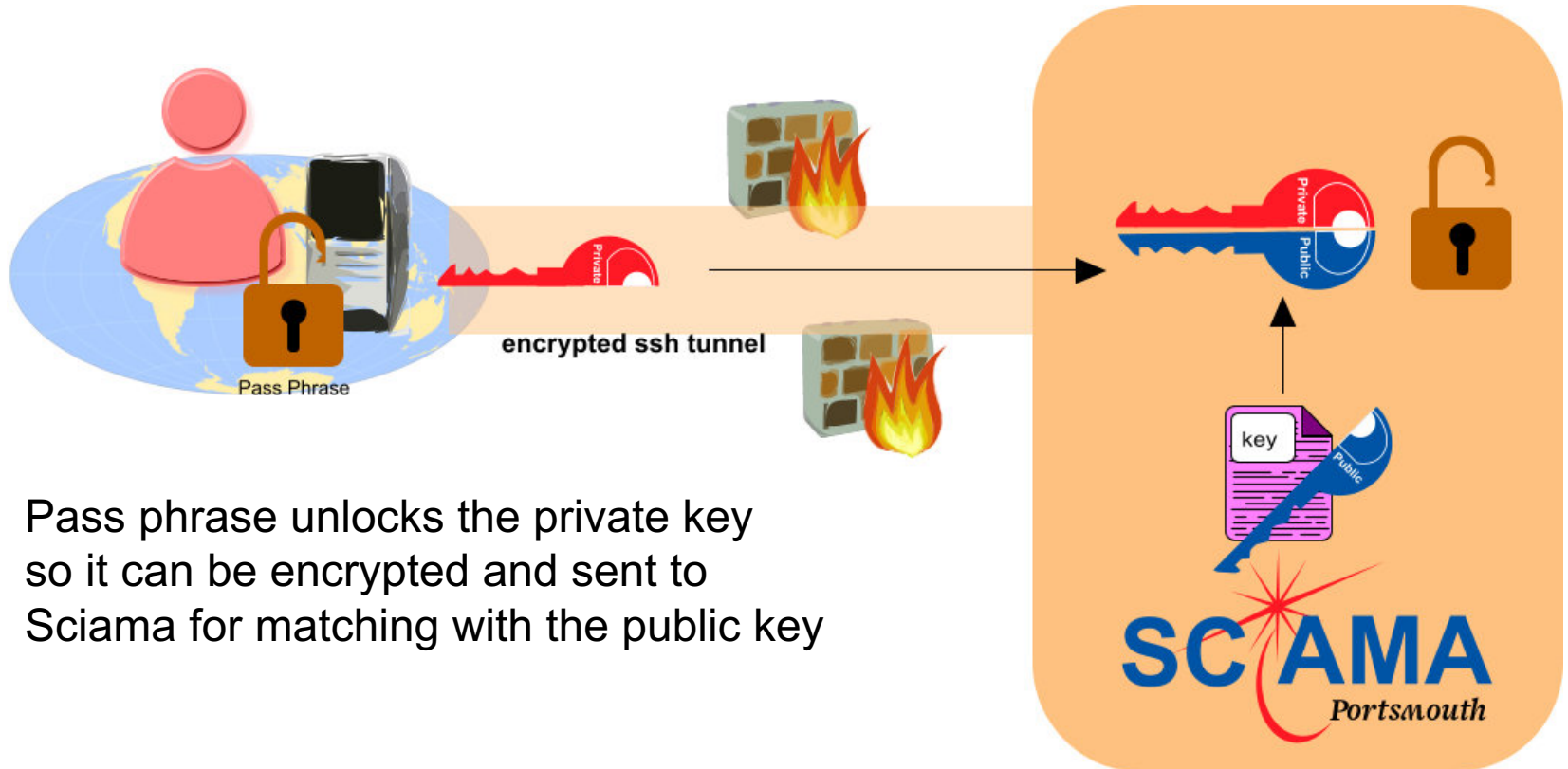
Example public key. You can cut and paste into Emails etc.

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEA4d
CxHdxl6R5k5ZZbWiMRQC2cgC4W9sK4P
svJj3p4Jmt7sy1cdZPP2k8698RTexUi2Lxej
oH5v1HRCkWz8WsHHdbNLOwt/FN7e/FA
91xy/UrO7VdBgEndN3DmYZ1cLK9Sq01n
wsw6H0hUL0k98+Qfc10Hoh/+QHTmll+
EXt2hKRdnda2GAw148zXOPCXL1EnL4fR
f90fe9nv9DGrQGM9s3epWMxBMEwU9fqv
boo+CtNtYOCx20OecSZ61sDpKyPefrihPJ
ACBwcBHBSvCdxpfV6NO+0ZUVpvFU0zK
T1oJtswKIVJjcxRJZnekttNUT5ttyfHcrNM5
Xg/HRqgW2Dqa7Q==
```

What you know and what you have.



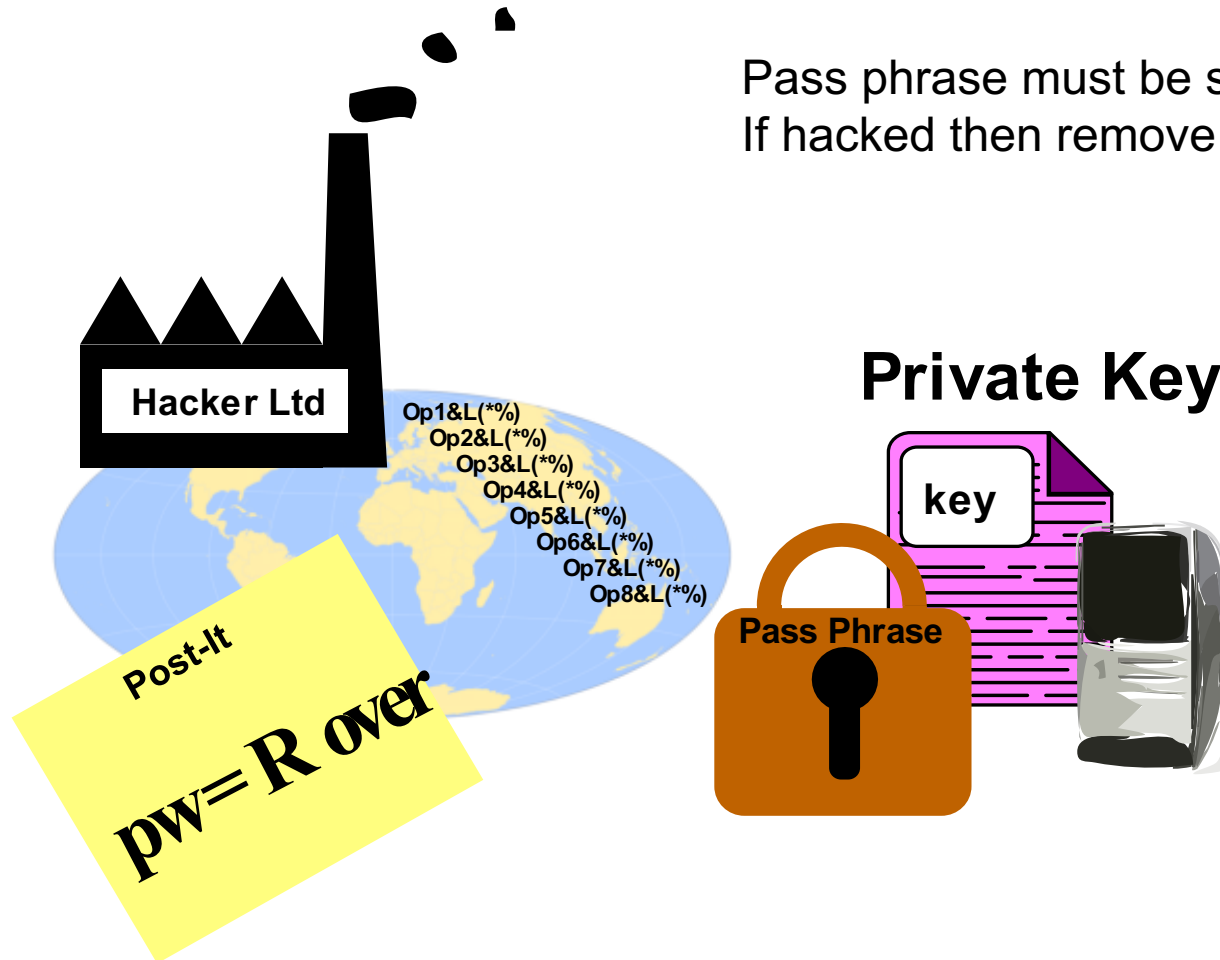
Public & Private + PassPhrase



Pass phrase unlocks the private key so it can be encrypted and sent to Sciama for matching with the public key

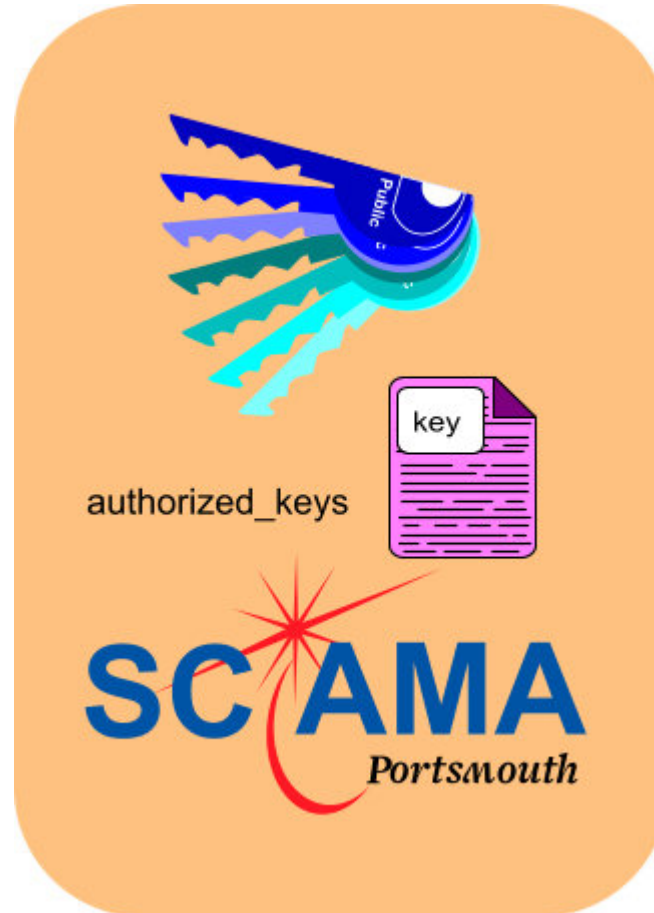
Private key can be hacked

Pass phrase must be sensible.
If hacked then remove Public keys.



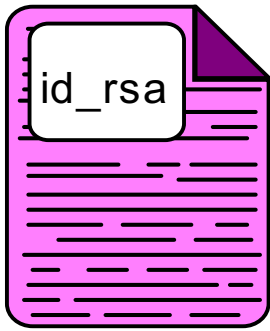
On Sciama you may have several public keys concatenated

A private key may be used on more than one desktop / laptop.



Linux / MAC = ssh-keygen

```
burtong@osboxes: ~  
File Edit View Search Terminal Help  
Rhythmbox  
burtong@osboxes:~$  
burtong@osboxes:~$ ssh-keygen -t rsa  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/burtong/.ssh/id_rsa):  
Created directory '/home/burtong/.ssh'.  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/burtong/.ssh/id_rsa.  
Your public key has been saved in /home/burtong/.ssh/id_rsa.pub.  
The key fingerprint is:  
SHA256:2MTKd1MxNd40BLd8yY5HQrZJ/YgVBVMkL48b/Wp1A/w burtong@osboxes  
The key's randomart image is:  
+----[RSA 2048]-----+  
|  
| o*@X=|  
| . ++B0+|  
| o o*B=|  
| . = ..O*=o|  
| + S o .=oo|  
| . . . .E+|  
| ..+|  
| ..|  
| ..|  
+----[SHA256]-----+  
burtong@osboxes:~$
```

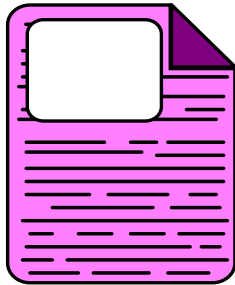


Private key kept safe on desktop
in `$HOME/.ssh/id_rsa`

Pass Phrase



id_rsa.pub



Public key concatenated in
\$HOME/.ssh/authorized_keys
on Sciamia

```
---- BEGIN SSH2 PUBLIC KEY ----Comment: "rsa-key-  
20171002" AAAAB3NzaC1yc2EAAAABJQAAAQEAsuuVNO7aNI90  
Uu5cn9al05I9XOTR18Ee5mRTduJwPftQKxnPRdPsJx4XJfq3WsG  
X7lkXwFW/VMnPNgNntGsikb3DE9IhTkgdAVT73Vqs+rpFyTmGR  
QU0E4hDFtCkgQgBnNweQAtQKj34mBi3qZl1hbLf3SZt56CKvqlxz  
ulENA0IiHu86J6/A/gloLkbKFlasAPbWS/w6tHfe2VRw3OHclcrubt  
ghgkbvELkr15z5MRllhTCCYaLwThJytzGIUkhcgd79be3UEnkszs22  
Qk6LqjjAXx59hO6CkWtoLchAsPKap2n6wrsDEdfxlhsroWvyyy0M  
dFiILDxFJg7vs+aQ===== END SSH2 PUBLIC KEY ----
```



Can be sent to other
systems

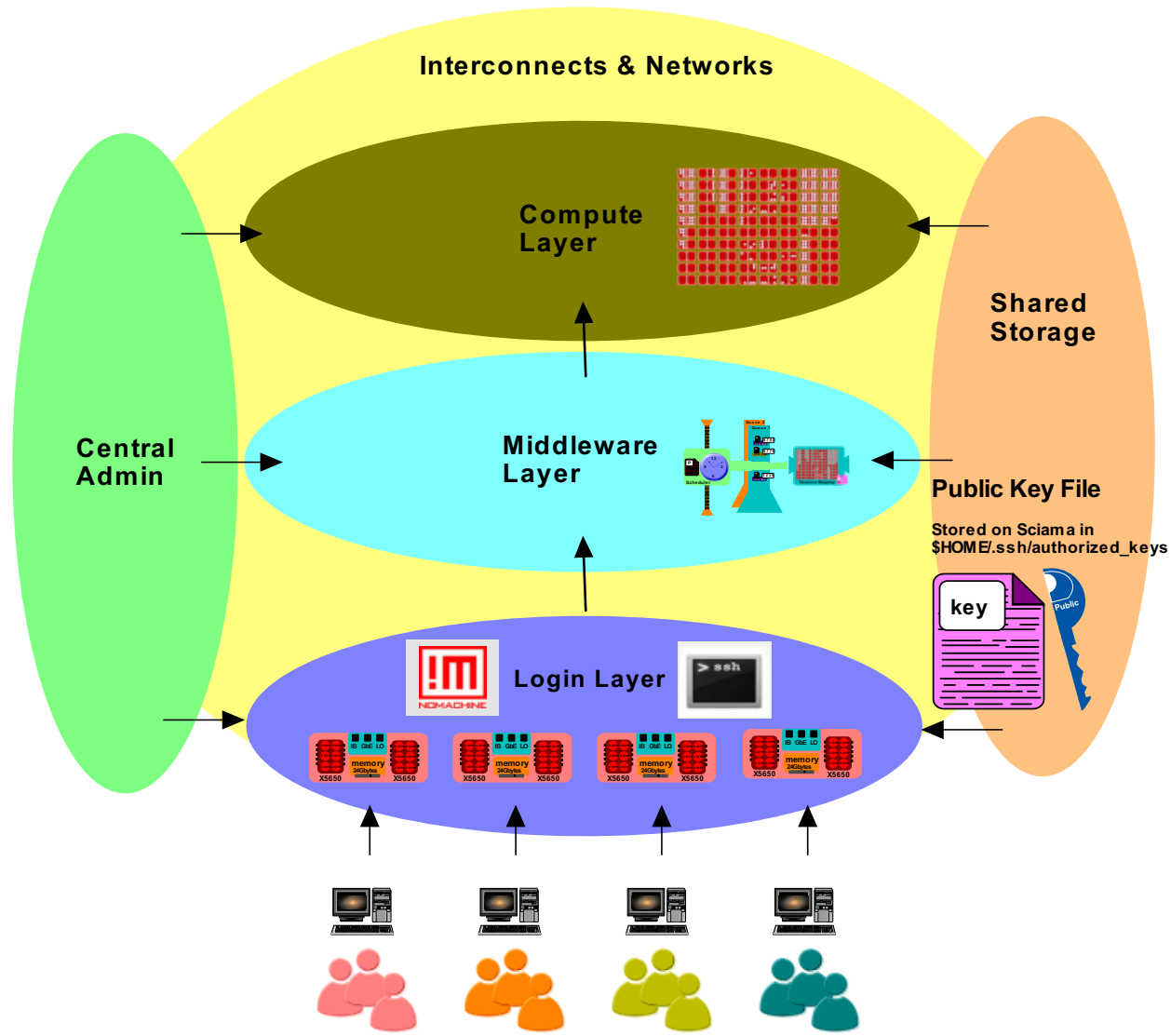


If you have passwd access ssh-copy-id

```
burtong@osboxes: ~  
File Edit View Search Terminal Help  
burtong@osboxes:~$ ssh-copy-id burtong@login8.sciama.icg.port.ac.uk  
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/burtong/.ssh/id_rsa.pub"  
The authenticity of host 'login8.sciama.icg.port.ac.uk (148.197.10.71)' can't be established.  
RSA key fingerprint is SHA256:zELprgvBZmyQRQ5/6/a58e3e660bR3lJZItu18pnZcg.  
Are you sure you want to continue connecting (yes/no)? yes  
/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  
burtong@login8.sciama.icg.port.ac.uk's password:  
  
Number of key(s) added: 1  
  
Now try logging into the machine, with: "ssh 'burtong@login8.sciama.icg.port.ac.uk'"  
and check to make sure that only the key(s) you wanted were added.  
  
burtong@osboxes:~$
```

Same key on each login server

(\$HOME/.ssh is the same)



First time will warn you about host and prompt for pass phrase

```
burtong@login7:~  
File Edit View Search Terminal Help  
  
burtong@osboxes:~$ ssh burtong@login7.sciama.icg.port.ac.uk  
The authenticity of host 'login7.sciama.icg.port.ac.uk (148.197.10.70)' can't be established.  
RSA key fingerprint is SHA256:5dK0hH+HibMddvrSzJn9vm0Chx8Q/hFwPz9WM9jRACI.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'login7.sciama.icg.port.ac.uk,148.197.10.70' (RSA) to the list of known hosts.  
Enter passphrase for key '/home/burtong/.ssh/id_rsa':  
Last login: Sat Apr 28 17:28:18 2018 from host86-189-176-148.range86-189.btcentralplus.com  
  
+++++  
Welcome to Alces Software HPC Stack For Linux  
Based on Scientific Linux 6.5  
+++++  
  
@@@@@@@@@ PLEASE NOTE THAT DATA ON SCIAMA IS NOT BACKED UP @@@@@@@@@@  
  
TIPS:  
  
'module avail' - show available application environments  
'module add <modulename>' - add a module to your current environment  
  
'qstat' - show summary of running jobs  
  
(Training)[burtong@login7(sciama) ~]$
```


From then on will prompt for pass phrase (local challenge)

```
burtong@login7:~  
File Edit View Search Terminal Help  
Connection to login7.sciama.icg.port.ac.uk closed.  
burtong@osboxes:~$ ssh burtong@login7.sciama.icg.port.ac.uk  
Enter passphrase for key '/home/burtong/.ssh/id_rsa':  
Last login: Sun Apr 29 10:54:44 2018 from host31-53-183-199.range31-53.btcentra  
lplus.com  
  
+++++  
Welcome to Alces Software HPC Stack For Linux  
Based on Scientific Linux 6.5  
+++++  
  
@@@@@@@@ PLEASE NOTE THAT DATA ON SCIAMA IS NOT BACKED UP @@@@@@@@@@  
  
TIPS:  
  
'module avail'           - show available application environments  
'module add <modulename>' - add a module to your current environment  
  
'qstat'                  - show summary of running jobs  
  
(Training)[burtong@login7(sciama) ~]$
```

Ssh-agent enters pass phrase for you

```
burtong@login7:~
File Edit View Search Terminal Help
burtong@osboxes:~$
burtong@osboxes:~$ eval 'ssh-agent bash'
burtong@osboxes:~$ ssh-add
Enter passphrase for /home/burtong/.ssh/id_rsa:
Identity added: /home/burtong/.ssh/id_rsa (/home/burtong/.ssh/id_rsa)
burtong@osboxes:~$ ssh burtong@login7.sciama.icg.port.ac.uk
Last login: Sun Apr 29 10:56:37 2018 from host31-53-183-199.range31-53.btcentra
lplus.com

+++++
Welcome to Alces Software HPC Stack For Linux
Based on Scientific Linux 6.5
+++++

@@@@@@@@@ PLEASE NOTE THAT DATA ON SCIAMA IS NOT BACKED UP @@@@@@@@@@

TIPS:

'module avail' - show available application environments
'module add <modulename>' - add a module to your current environment

'qstat' - show summary of running jobs

(Training)[burtong@login7(sciama) ~]$
```

Common Problem

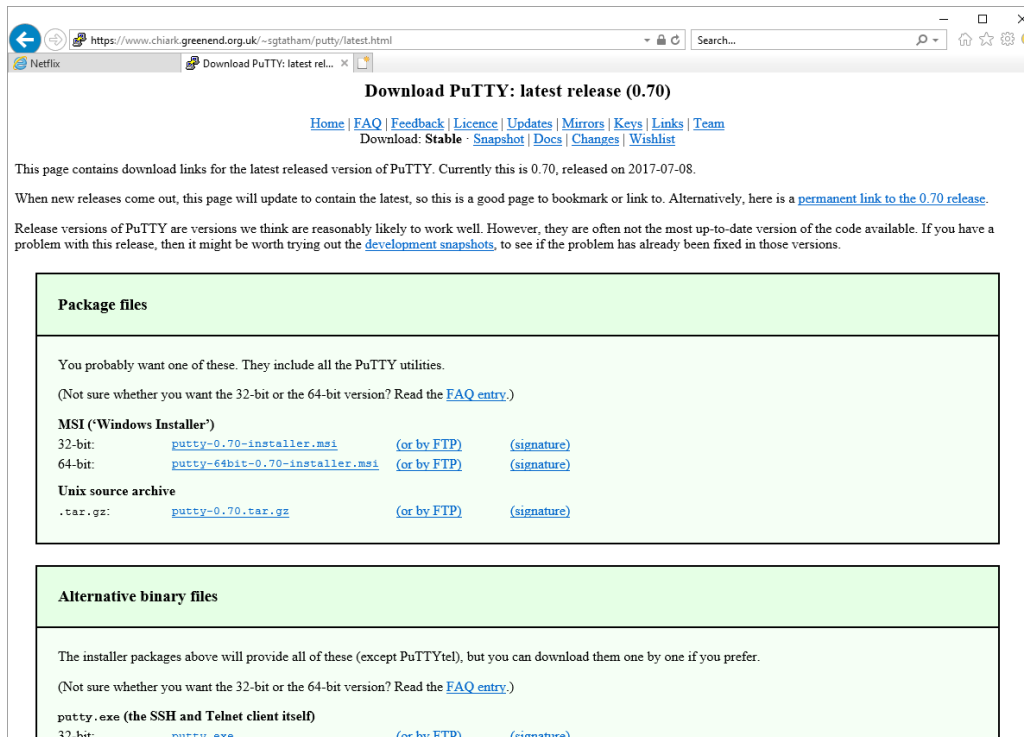
```
(Training)[burtong@login6(sciama) ~]$ssh login7
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@
@  WARNING: REMOTE HOST IDENTIFICATION HAS
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@
```

Login7 needs to be removed from the \$HOME/.ssh/known_hosts file on the client

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
ac:f6:31:0c:ac:b2:76:f1:2c:bc:40:1c:43:71:e4:62.
Please contact your system administrator.
Add correct host key in /users/burtong/.ssh/known_hosts to get rid of this message.
Offending key in /users/burtong/.ssh/known_hosts:259
Password authentication is disabled to avoid man-in-the-middle attacks.
Keyboard-interactive authentication is disabled to avoid man-in-the-middle attacks.
Last login: Sat Apr 28 16:06:30 2018 from host86-189-176-148.range86-189.btcentralplus.com



Windows - Putty, Puttygen & Pageant



The screenshot shows a web browser window with the URL <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>. The page title is "Download PuTTY: latest release (0.70)". The page contains navigation links: [Home](#), [FAQ](#), [Feedback](#), [Licence](#), [Updates](#), [Mirrors](#), [Keys](#), [Links](#), [Team](#), [Download: Stable](#), [Snapshot](#), [Docs](#), [Changes](#), and [Wishlist](#). The main content area is titled "Package files" and contains the following text:

You probably want one of these. They include all the PuTTY utilities.
(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

MSI ('Windows Installer')

32-bit: [putty-0.70-installer.msi](#) (or by [FTP](#)) ([signature](#))
64-bit: [putty-64bit-0.70-installer.msi](#) (or by [FTP](#)) ([signature](#))

Unix source archive

.tar.gz: [putty-0.70.tar.gz](#) (or by [FTP](#)) ([signature](#))

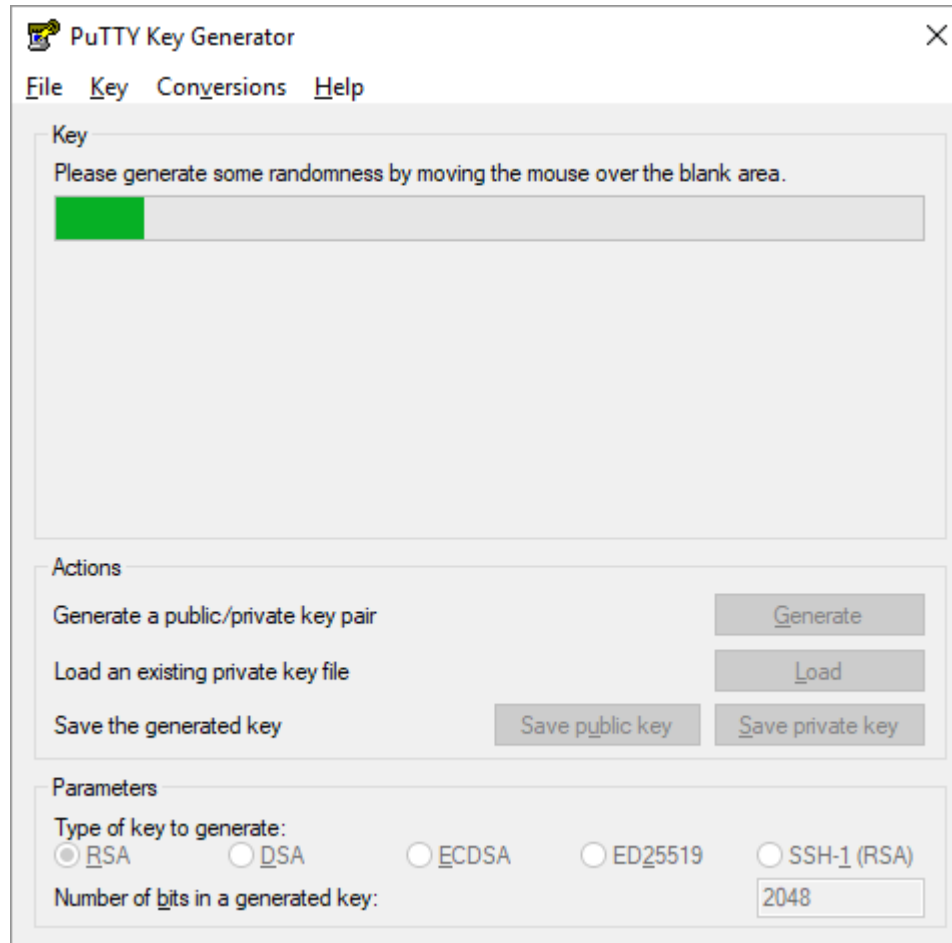
The "Alternative binary files" section contains the following text:

The installer packages above will provide all of these (except PuTTYtel), but you can download them one by one if you prefer.
(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

putty.exe (the SSH and Telnet client itself)

32-bit: [putty.exe](#) (or by [FTP](#)) ([signature](#))

Create key by random mouse movements



Putty Key Gen

The screenshot shows the PuTTY Key Generator window with the following details:

- Key:** A text area containing a long public key string: `ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEateob9KS90JX1SF7N+ICaxPwkd5+adtO+NVSIA2+0P1eYtqPar9Hrhe0KS0h1U3qV2F7UxwH6M/6Hky3YCDTvpkxo5+f8GxbUPd2ETrxebPBbETtHONtNTk3RvjW4TQIEjK0taOgRMolfMa1PWnW8BCRQoGOocu9mt8zXx5cobxwGDsSm/UGJ46LvKgGfXUiWi1GiA9nZS5QytXi4eNyl2N4UrpEaMoiVT`
- Key fingerprint:** `ssh-rsa 2048 15f6:0f:2c:ed:85:18:c0:9b:61:02:38:d5:23:52:2c`
- Key comment:** `rsa-key-20180430`
- Key passphrase:** A field with 10 dots.
- Confirm passphrase:** A field with 10 dots.
- Actions:** Buttons for `Generate`, `Load`, `Save public key`, and `Save private key`.
- Parameters:** `Type of key to generate:` with radio buttons for `RSA` (selected), `DSA`, `ECDSA`, `ED25519`, and `SSH-1 (RSA)`. `Number of bits in a generated key:` is `2048`.

Entering a pass phrase is mandatory

Save both public and private keys

Public key concatenated in \$HOME/.ssh/authorized_keys on Sciamia

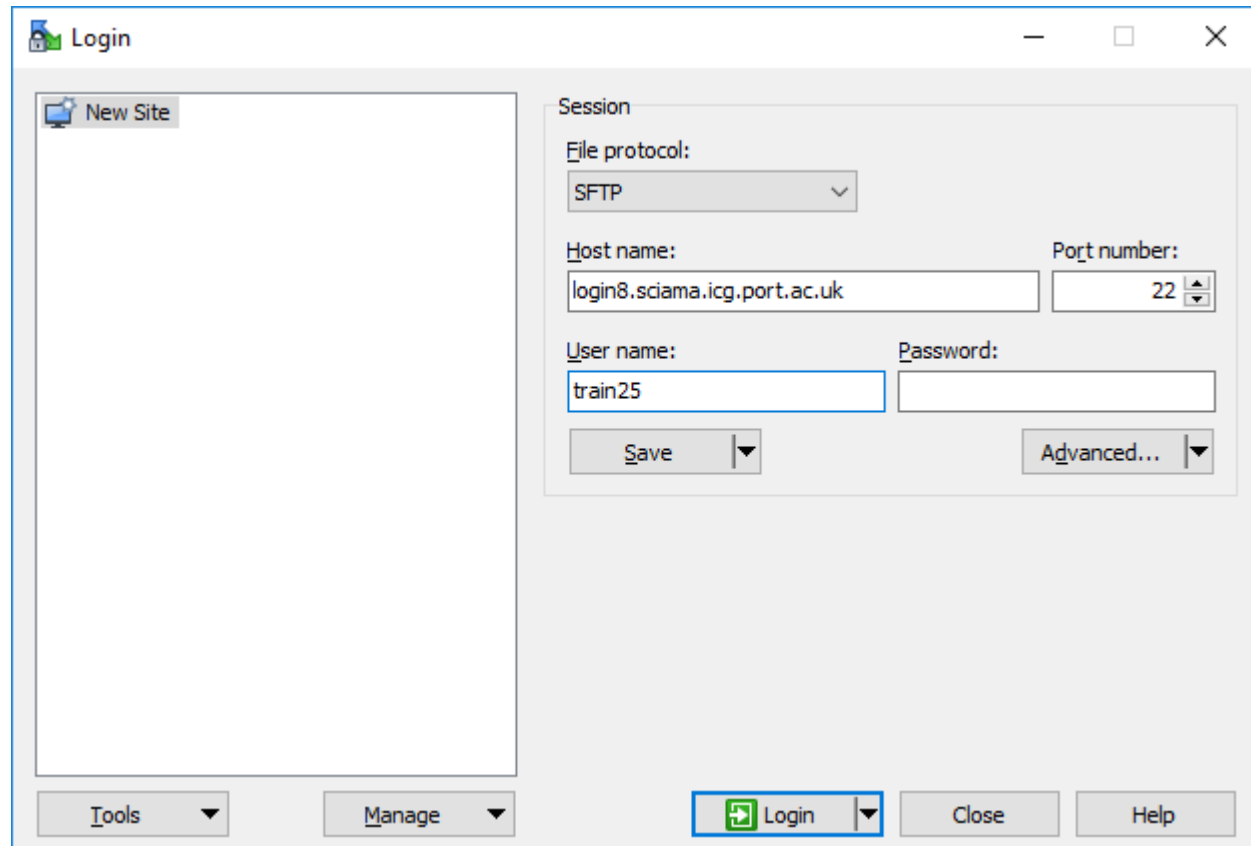
```
---- BEGIN SSH2 PUBLIC KEY ----Comment: "rsa-key-  
20171002"AAAAB3NzaC1yc2EAAAABJQAAAQEAAsuuVNO7aNI90  
Uu5cn9al05I9XOTR18Ee5mRTtduJwPftQKxnPRdPsJx4XJfq3WsG  
X7IkXwFW/VMnPNgNntGsikb3DE9IhTkgdAVT73Vqs+rpFyTmGR  
QU0E4hDFtCkgQgBnNweQAtQKj34mBi3qZl1hbLf3SZt56CKvqlxz  
ulENA0IiHu86J6/A/gloLkbKFiasAPbWS/w6tHfe2VRw3OHclcrubt  
ghgkbvELkr15z5MRllhTCCYaLwThJytzGIUkhcgd79be3UEnkszs22  
Qk6LqjjAXx59hO6CkWtoLchAsPKap2n6wrsDEdfxlhsroWvyyyy0M  
dFiILDxFJg7vs+aQ==----- END SSH2 PUBLIC KEY ----
```



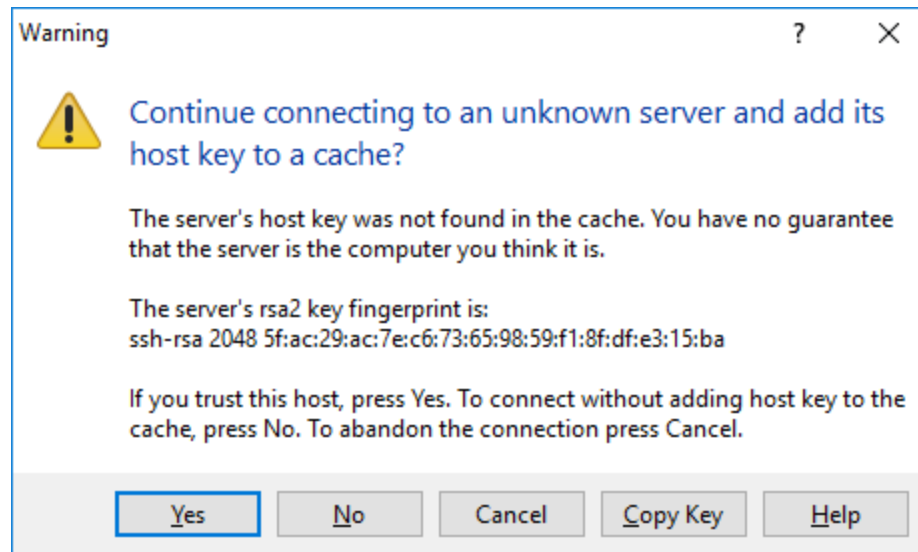
Can be sent to other
systems



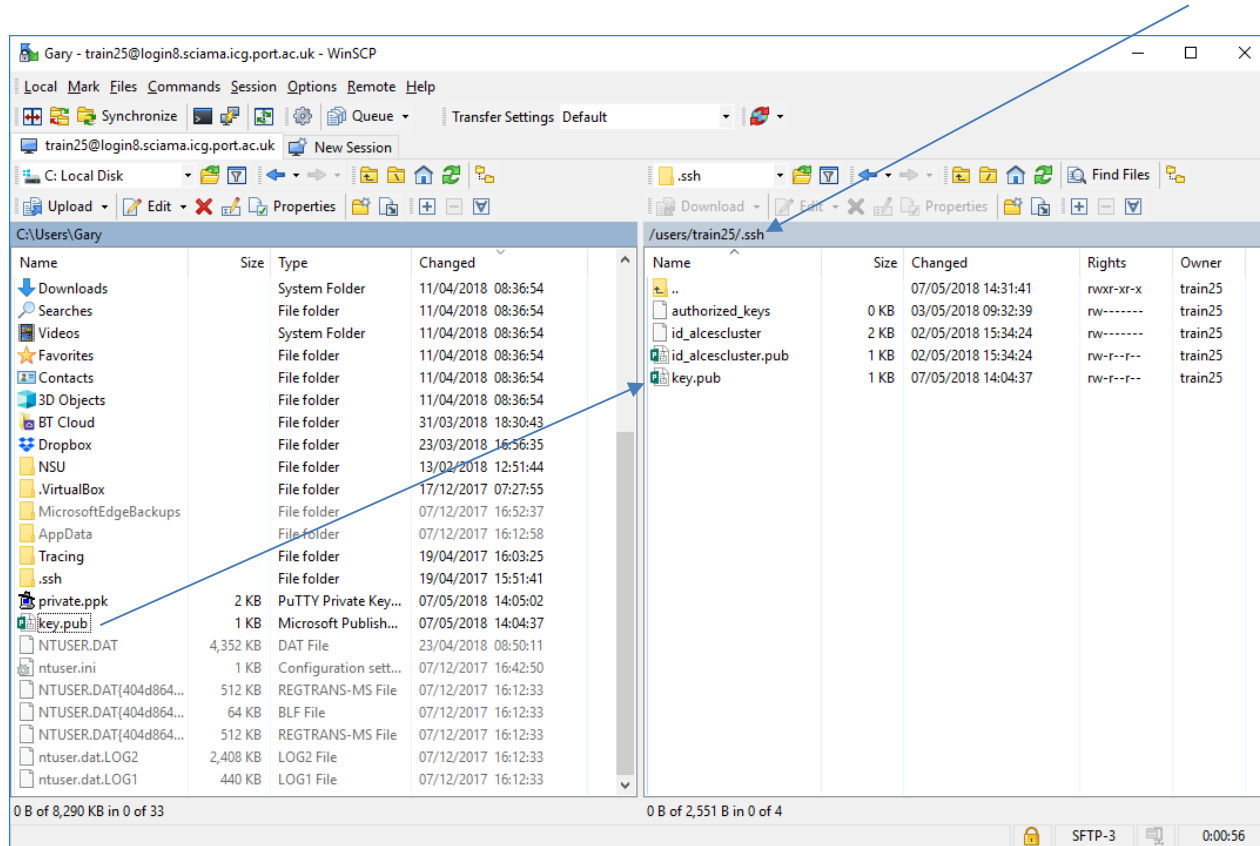
WinSCP connect to Login server with supplied pw



Acknowledge Warning



Transfer public key to .ssh directory



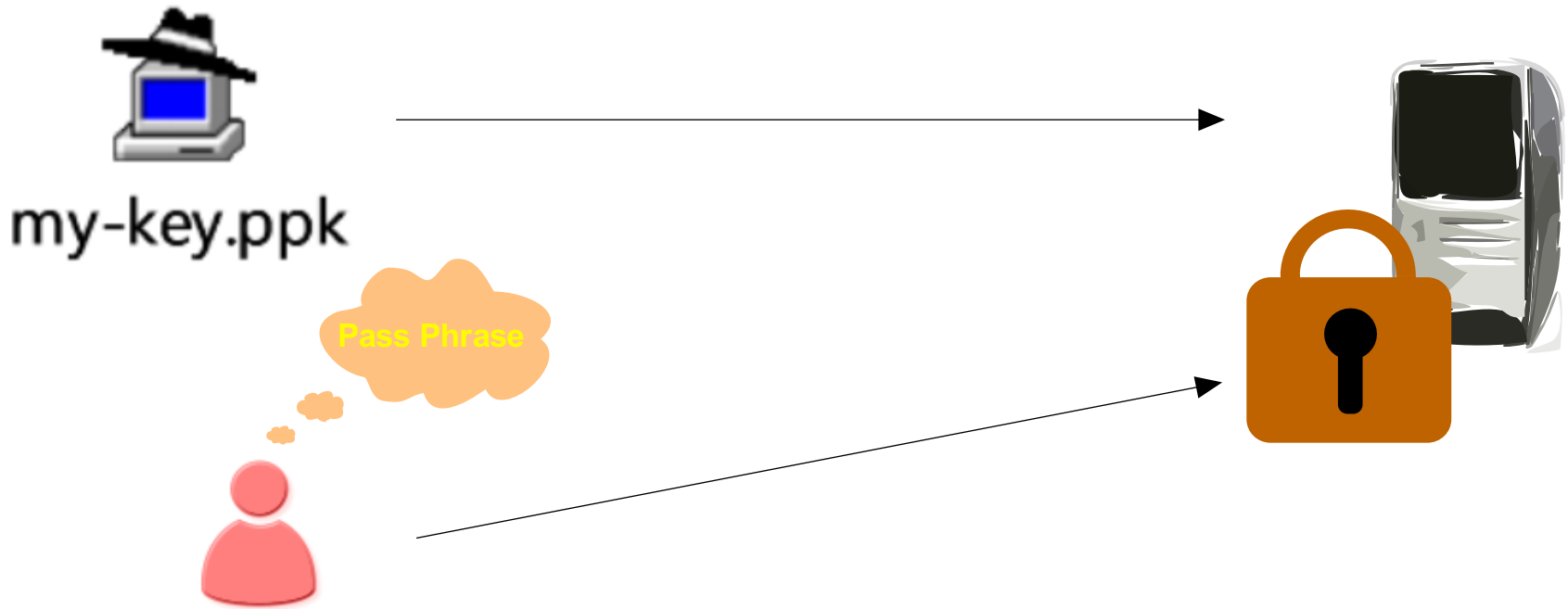
Login in with password and create an authorized_keys file

```
train25@login8:~/ssh
'module add <modulename>' - add a module to your current environment
'qstat' - show summary of running jobs

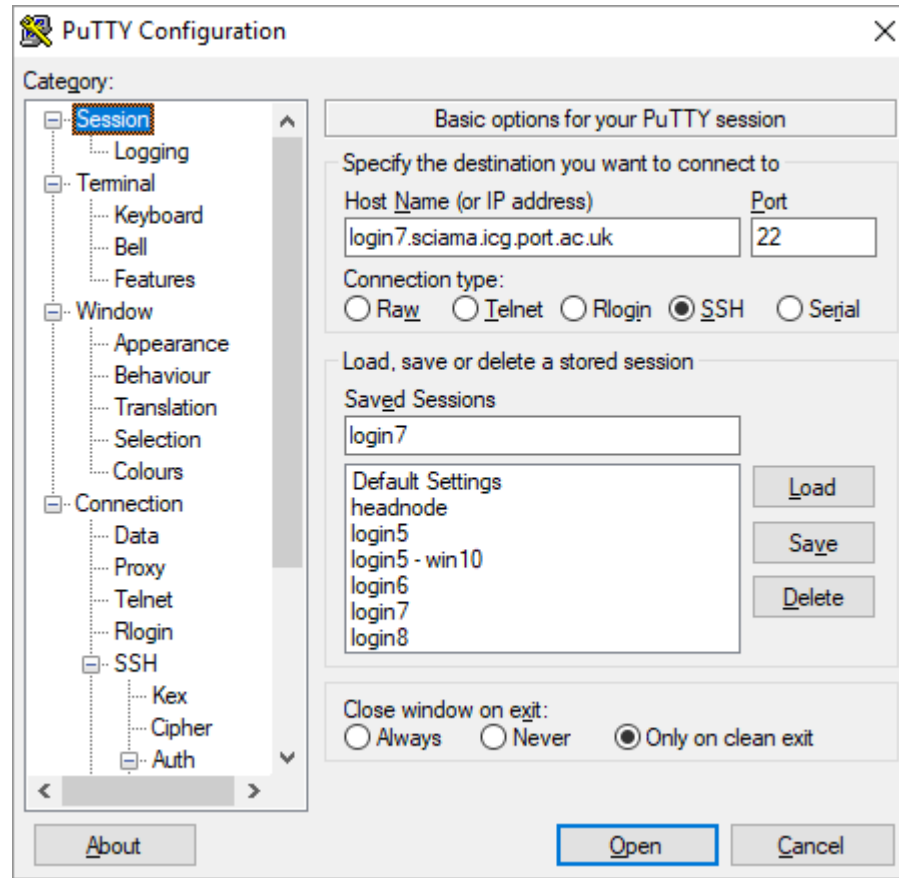
[train25@login8 (sciama) ~]$ cd .ssh
[train25@login8 (sciama) .ssh]$ ls
authorized_keys id_alcescluster id_alcescluster.pub ssh.pub
[train25@login8 (sciama) .ssh]$ more ssh.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20180507"
AAAAB3NzaClyc2EAAAABJQAAAQEA...
----- END SSH2 PUBLIC KEY -----

[train25@login8 (sciama) .ssh]$ more authorized_keys
ssh-rsa AAAAB3NzaClyc2EAAAABJQAAAQEA...
[train25@login8 (sciama) .ssh]$
```

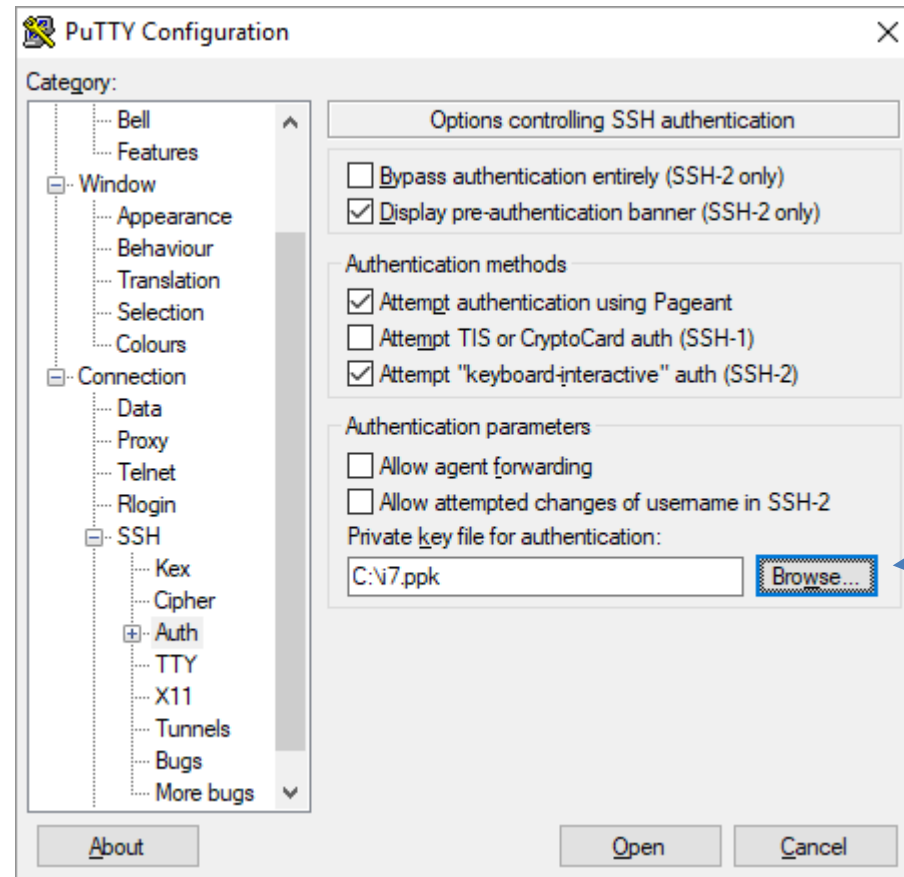
Private key kept safe on desktop



On Windows Putty is best connection tool.



Add key path to Putty ssh auth

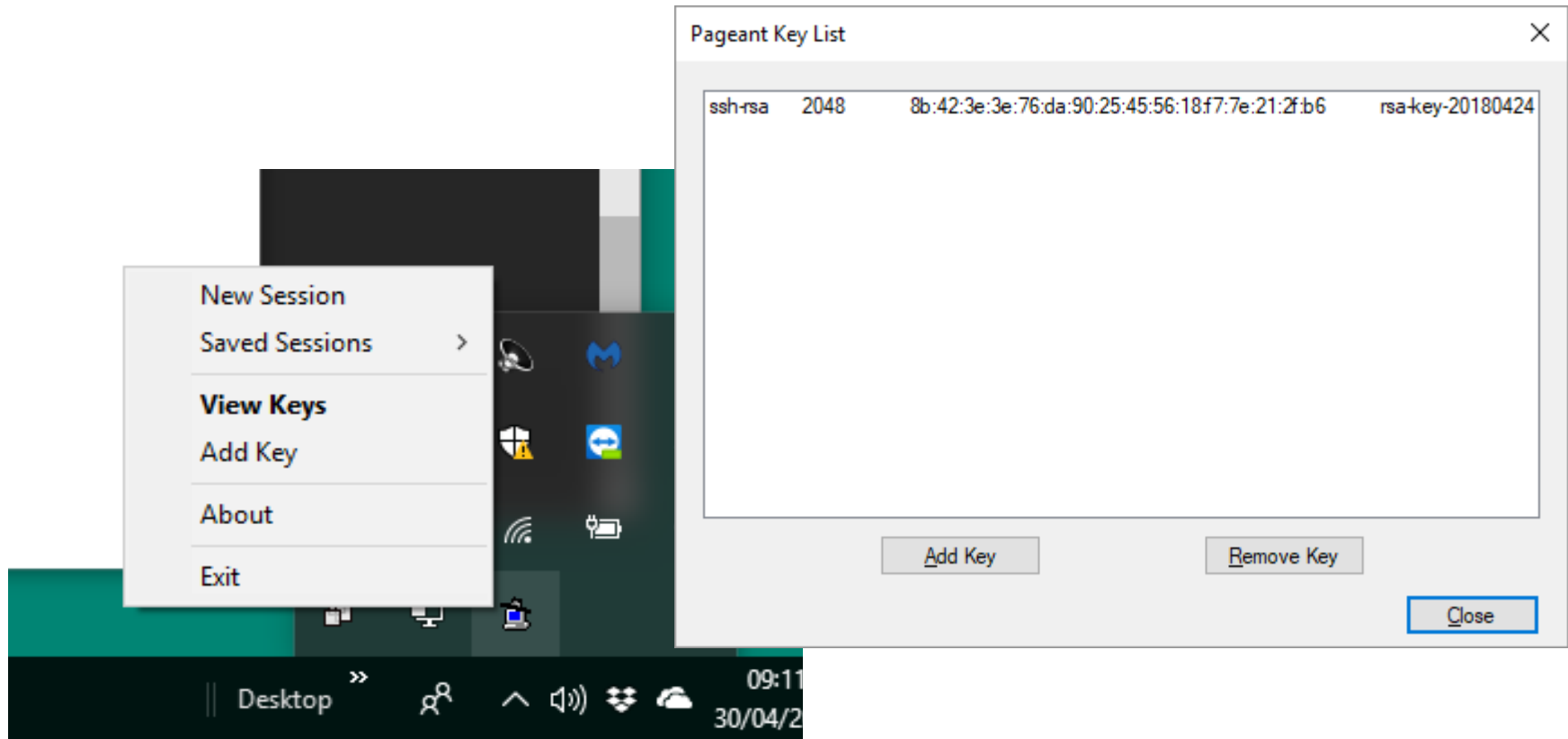


You will be prompted for pass phrase



```
login7.sciama.icg.port.ac.uk - PuTTY
login as: burtong
Authenticating with public key "rsa-key-20180424"
Passphrase for key "rsa-key-20180424": █
```

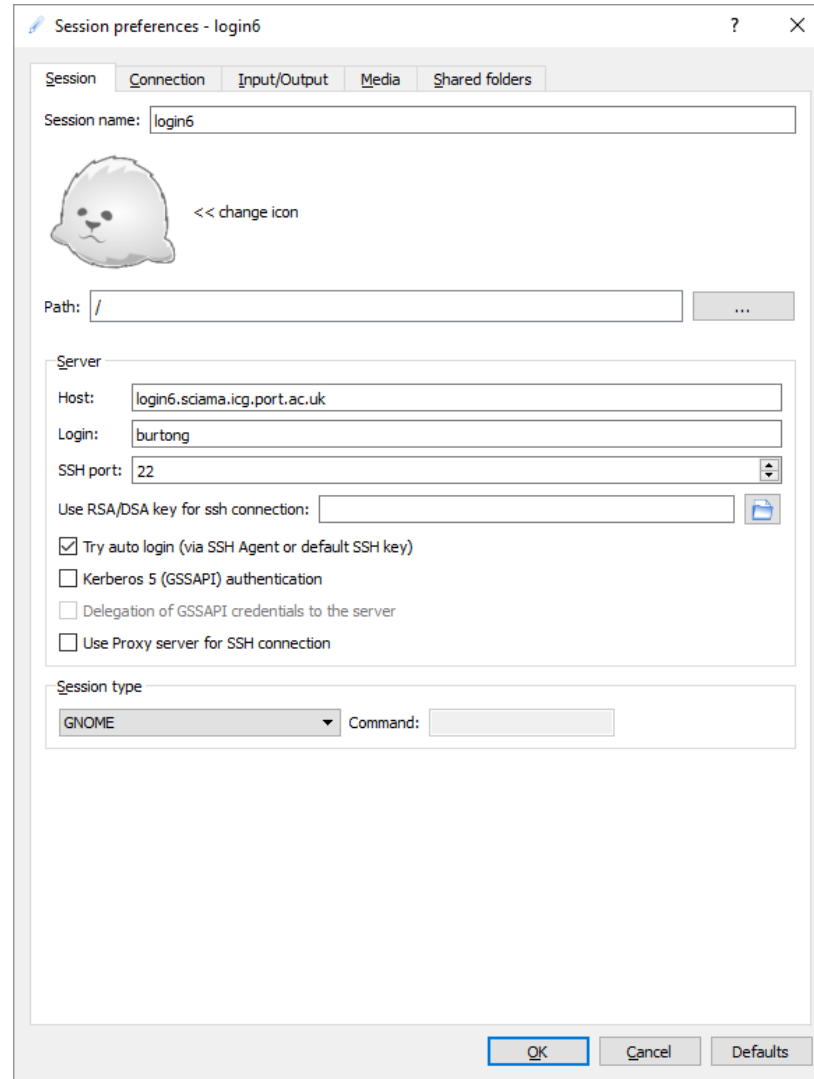
Use Pageant (agent) found in tool bar.



Using the agent gives you login with out typing the pass phrase

```
burtong@login7:~  
login as: burtong  
Authenticating with public key "rsa-key-20180424" from agent  
Last login: Sun Apr 29 11:15:59 2018 from host31-53-183-199.range31-53.btcentral  
plus.com  
  
+++++  
Welcome to Alces Software HPC Stack For Linux  
Based on Scientific Linux 6.5  
+++++  
  
@@@@@@@@@@ PLEASE NOTE THAT DATA ON SCIAMA IS NOT BACKED UP @@@@@@@@@@  
  
TIPS:  
  
'module avail'           - show available application environments  
'module add <modulename>' - add a module to your current environment  
  
'qstat'                 - show summary of running jobs  
  
(Training) [burtong@login7 (sciama) ~]$ █
```

X2go



Either have age

Nomachine

login8

NOMACHINE

Choose which authentication method you want to use.

- Password
Use password authentication.
- Private key
Use key-based authentication with a key you provide.
- Smart card
Use key-based authentication with a key stored on a PKCS11 smart card.
- Kerberos
Use Kerberos ticket-based authentication.

Settings

Settings

Settings

OK