

Public Key Authentication With PuTTY

These instructions apply to the PuTTY client on Windows. Help is also available through Start > All Programs > PuTTY > PuTTY Manual. If you encounter any problems, please send a note to research.support@ualberta.ca.

Contents

- [Preliminary Setup](#)
 - [Step 1](#)
 - [Step 2](#)
 - [Step 3](#)
- [Typical Usage](#)
- [Security Considerations](#)

Preliminary Setup

Setting up public key authentication to access a particular remote host is a one-time procedure comprising three steps.

Step 1

Generate a public/private key pair on your local desktop. From the Start menu, run Start > All Programs > PuTTY > PuTTYgen as illustrated below.



Fig. 1 Initial PuTTYgen window.

Click the Generate button. You will be prompted to move the mouse over the blank area to generate some randomness. Do so. Shortly thereafter, the program will generate the key and display the result (see Figure 2).

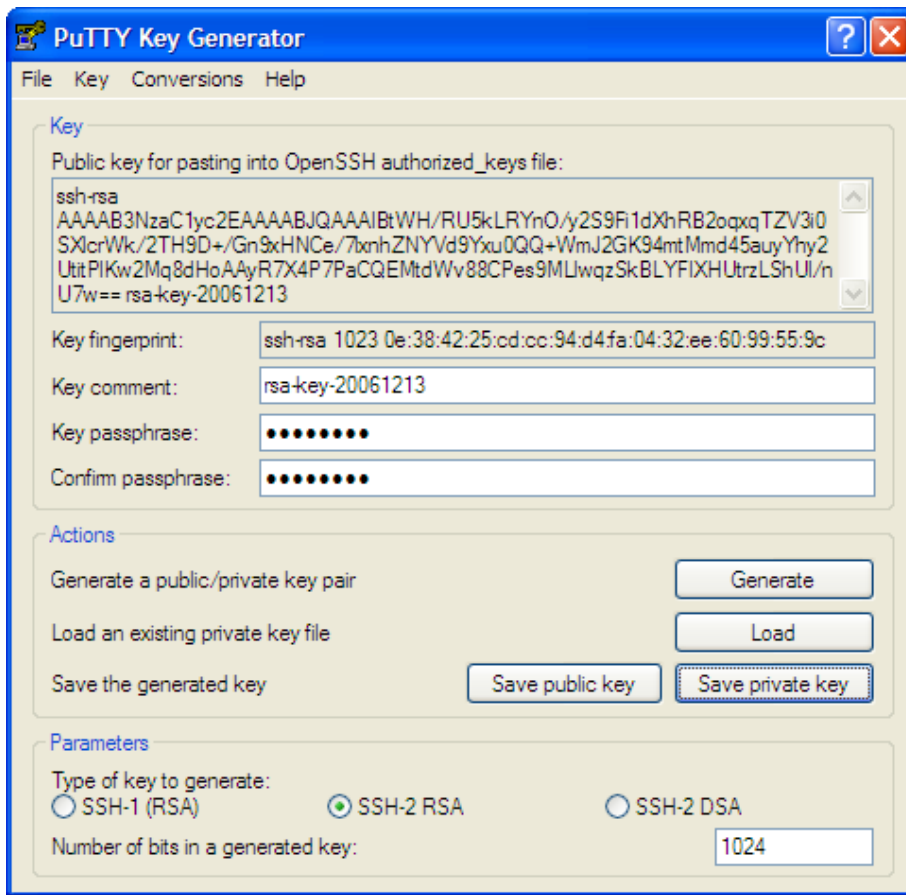


Fig. 2 After keys have been generated.

Enter a passphrase in the "Key passphrase" and "Confirm passphrase" boxes. Your CCID password makes a good choice since you have probably already committed it to memory and it has withstood password cracking tests. However, the PuTTY documentation recommends an actual phrase of 10 to 30 characters with word breaks, mixed case, numbers, and non-alphanumeric characters, for example, "DoN't (expect snow)^july." Instead of trying to create a good passphrase on your own, seriously consider the recommendations posted on www.diceware.com.

Under no circumstances should you leave these fields blank.

Select *all* of the text in the box labeled "Public key for pasting into OpenSSH authorized_keys file" (near the top of the window) by dragging the cursor. Right-click over the selection and choose Copy. Finally, click the "Save private key" button to save the private key to a file (Figure 3).

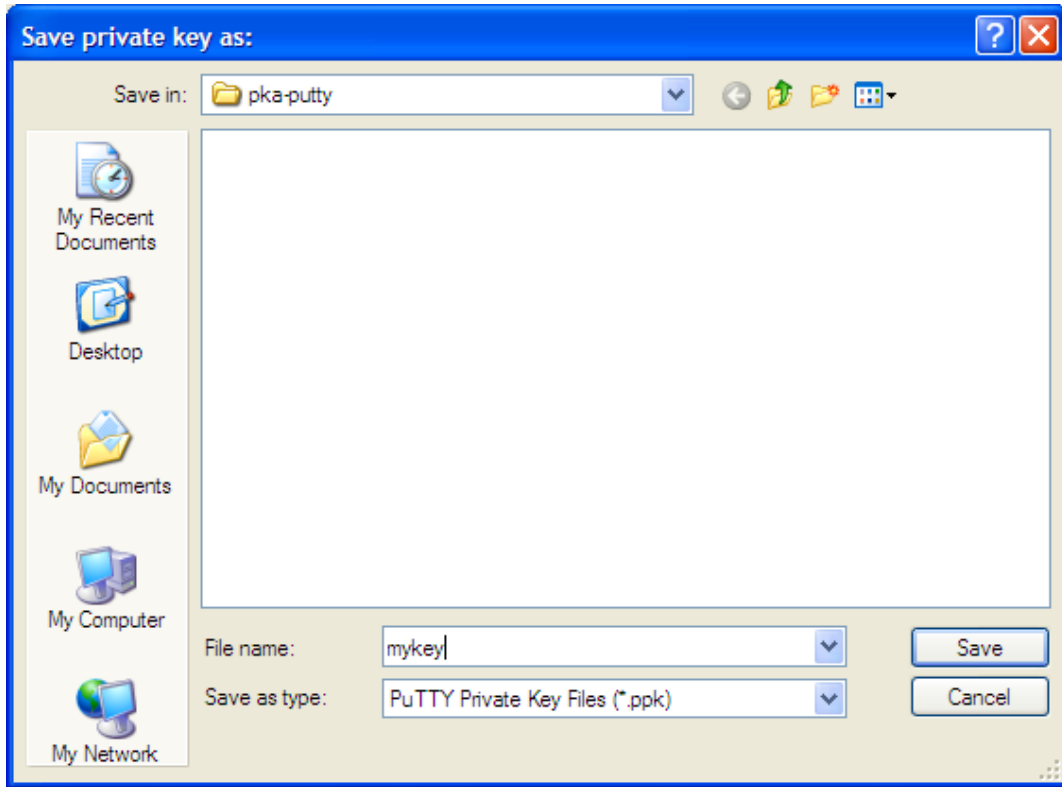


Fig. 3 Saving the private key in file mykey.ppk.

The private key must be kept secret. Accordingly, the contents of the file are encrypted using the passphrase, and you should pick a file location that is accessible only to you.

If you share your computer and you do not have a separate account (id) with private disk space, do not use public key authentication. If in doubt, do not use public key authentication.

You can recover the public key from the private key with PuTTYgen by clicking the Load button. You can not recover the private key from the public key however.

Step 2

Install the public key on the remote host to which you want to connect. Do this by pasting the public key from the Clipboard into the the `authorized_keys` file, which is located in the `.ssh` directory in your home directory on the remote host. Figure 3 shows the vi editor being used for this purpose.

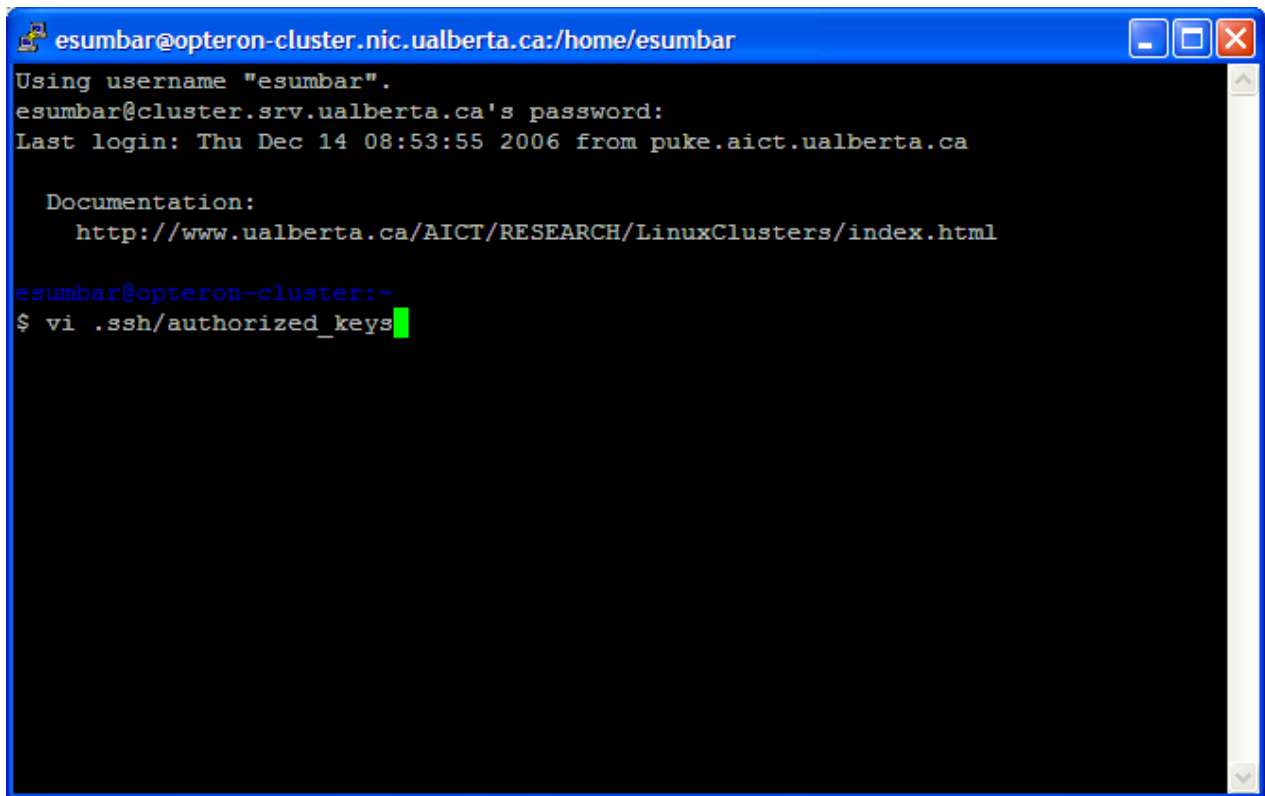


Fig. 4 Editing `.ssh/authorized_keys` with vi.

Type `g` on the keyboard to go to the end of the file. Enter insert mode on a new line by typing an `o` (lowercase oh), then right-click to paste the public key. The result is shown in Figure 4.

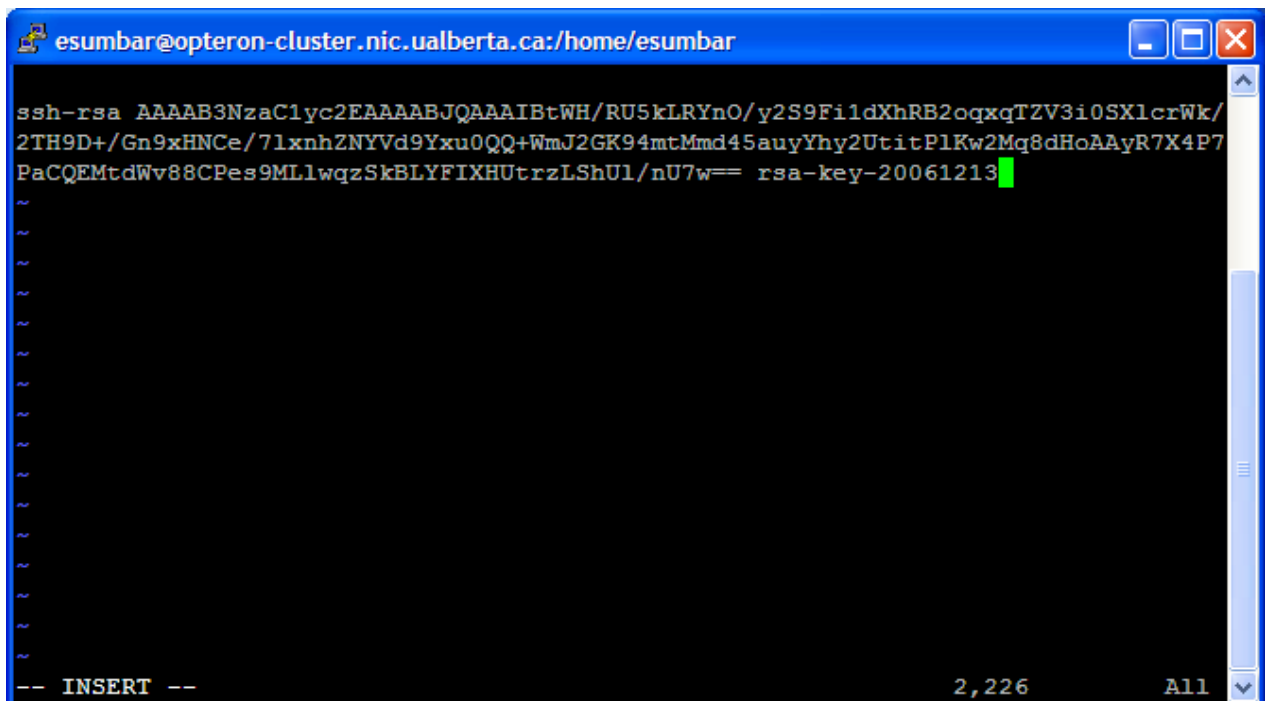


Fig. 5 After pasting the public key.

Press the `ESC` key to exit insert mode. And finally, type `:wq` to save the changes to the file and exit the editor. Repeat this procedure to install the same public key on as many additional remote hosts as you like.

The private key is not installed on any remote host.

Step 3

Verify that public key authentication works. Basic public key authentication is enabled for a particular session in the Connection > SSH > Auth window. You must load the session profile (Figure 6) before configuring the Auth window (Figure 7).

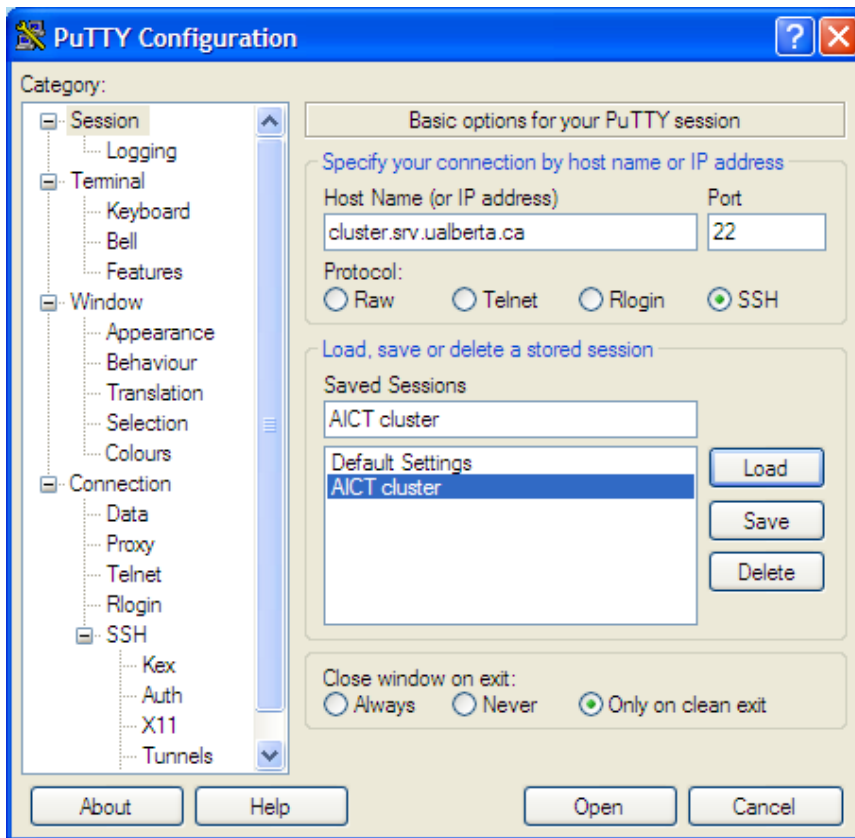


Fig. 6 Load the appropriate session profile.

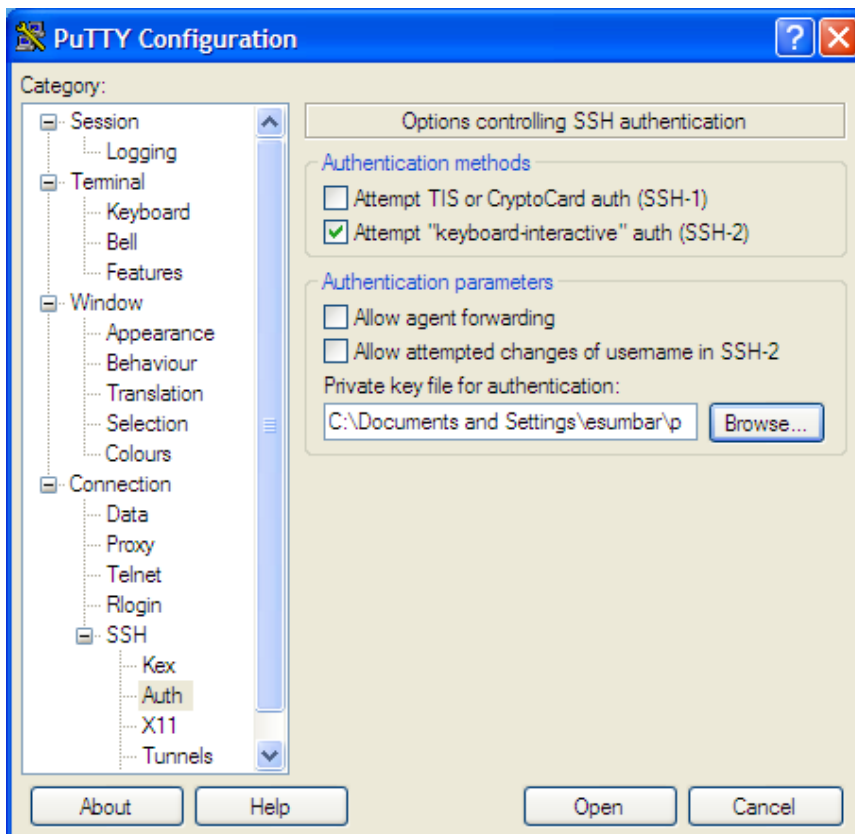
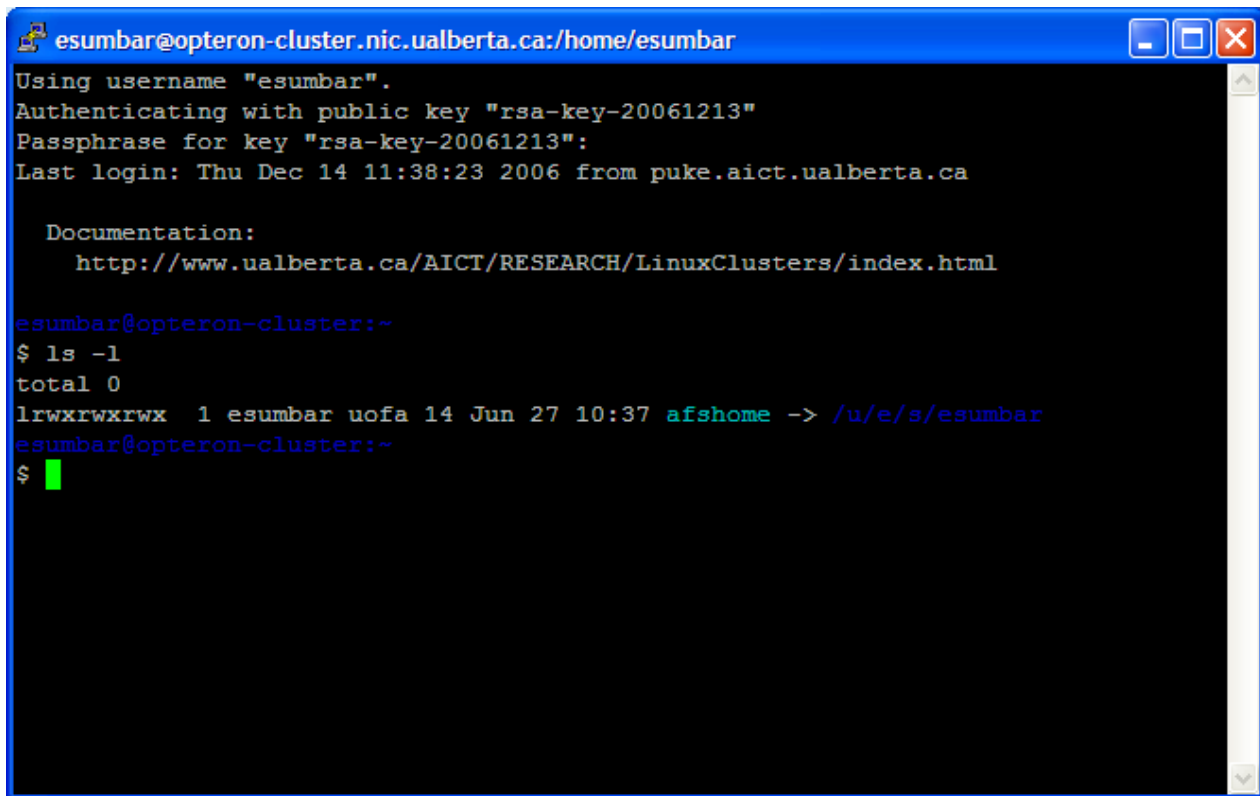


Fig. 7 Connection > SSH > Auth window.

Browse to select mykey.ppk in the "Private key file for authentication" text box. Be sure to go back to the Session window and click Save to update the profile. The session will use public key authentication as demonstrated in Figure 8.



```

esumbar@opteron-cluster.nic.ualberta.ca:/home/esumbar
Using username "esumbar".
Authenticating with public key "rsa-key-20061213"
Passphrase for key "rsa-key-20061213":
Last login: Thu Dec 14 11:38:23 2006 from puke.aict.ualberta.ca

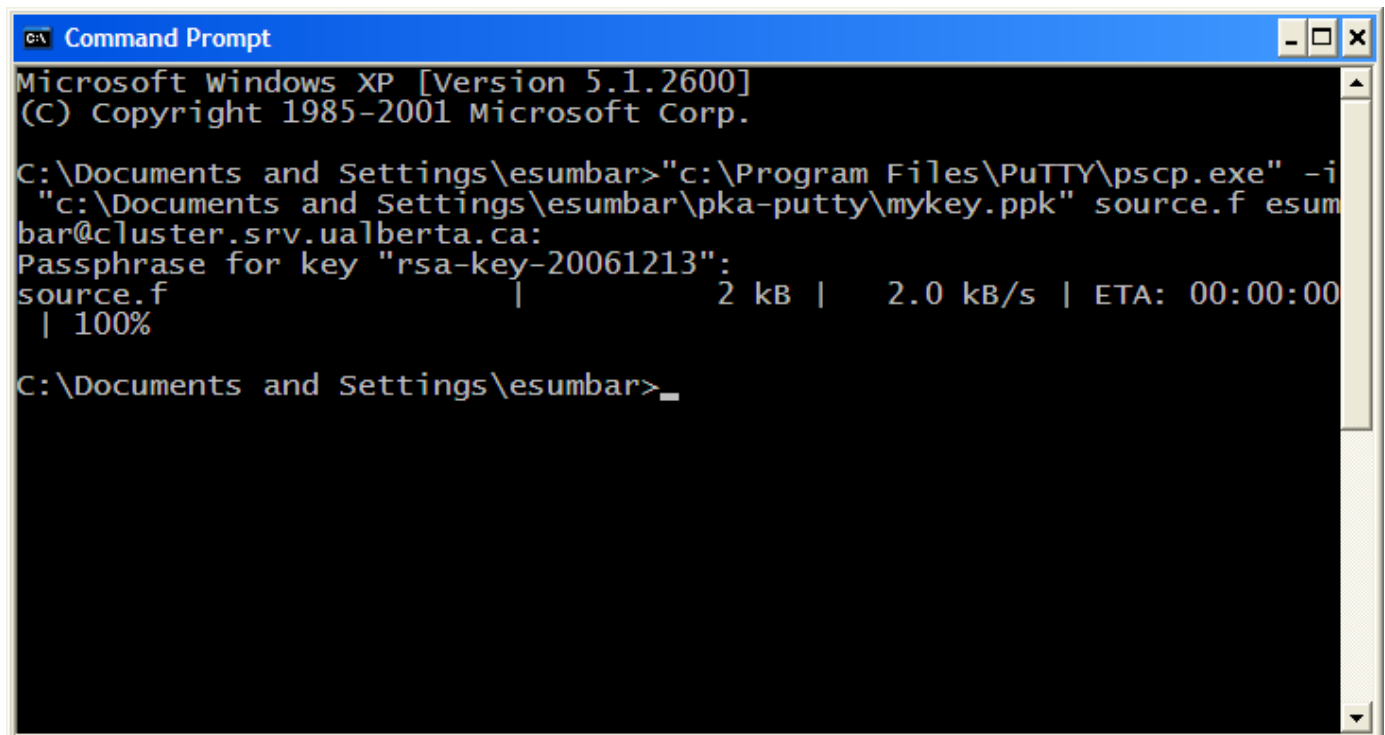
Documentation:
  http://www.ualberta.ca/AICT/RESEARCH/LinuxClusters/index.html

esumbar@opteron-cluster:~
$ ls -l
total 0
lrwxrwxrwx  1 esumbar uofa 14 Jun 27 10:37 afshome -> /u/e/s/esumbar
esumbar@opteron-cluster:~
$

```

Fig. 8 Logging in using basic public key authentication.

To invoke basic public key authentication for file transfers with pscp.exe, use the `-i` flag on the command line and specify mykey.ppk as the flag's argument.



```

C:\> Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\esumbar> "c:\Program Files\PuTTY\pscp.exe" -i
"c:\Documents and Settings\esumbar\pka-putty\mykey.ppk" source.f esum
bar@cluster.srv.ualberta.ca:
Passphrase for key "rsa-key-20061213":
source.f                               2 kB |  2.0 kB/s | ETA: 00:00:00
| 100%

C:\Documents and Settings\esumbar> _

```

Fig. 9 File transfer using basic public key authentication.

During either login or file transfer, supplying the passphrase when prompted decrypts the private key on the fly for use in the authentication process. If you see a password prompt

instead of a passphrase prompt, the administrators of the remote host may have disallowed public key authentication. Some sites take this step to prevent the use of unencrypted private keys (generated with a null passphrase), which pose a security threat.

Typical Usage

At first glance, basic public key authentication offers no advantages since a passphrase is always required. However, single signon can be achieved by setting up the PuTTY authentication agent, Pageant (pronounced page-ant).

Starting Pageant (Start > All Programs > PuTTY > Pageant) puts an icon in the system tray. Right-click on the icon and choose "Add Key" as illustrated below.

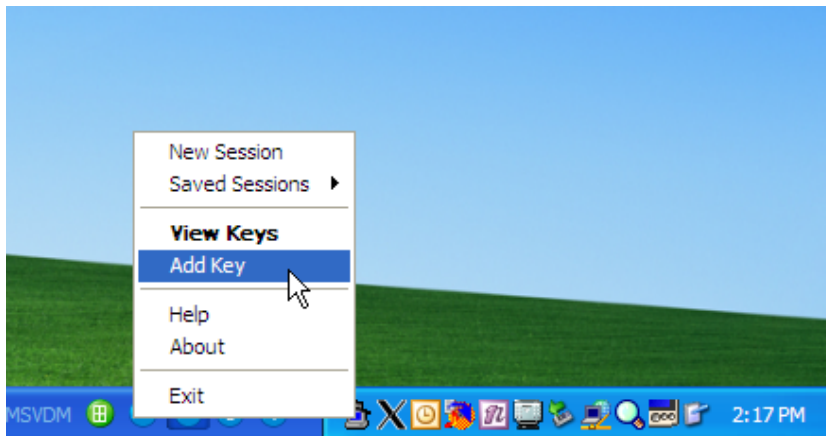


Fig. 10 Adding a key to Pageant.

When the "Select Private Key File" dialog appears, find mykey.ppk. You will be prompted for the passphrase so that Pageant can store the unencrypted private key in memory to use in authentication. Remove mykey.ppk from the "Private key file for authentication" text box in the Connections > SSH > Auth window for the session profile. All subsequent logins and file transfers will be authenticated by Pageant (Figure 11).

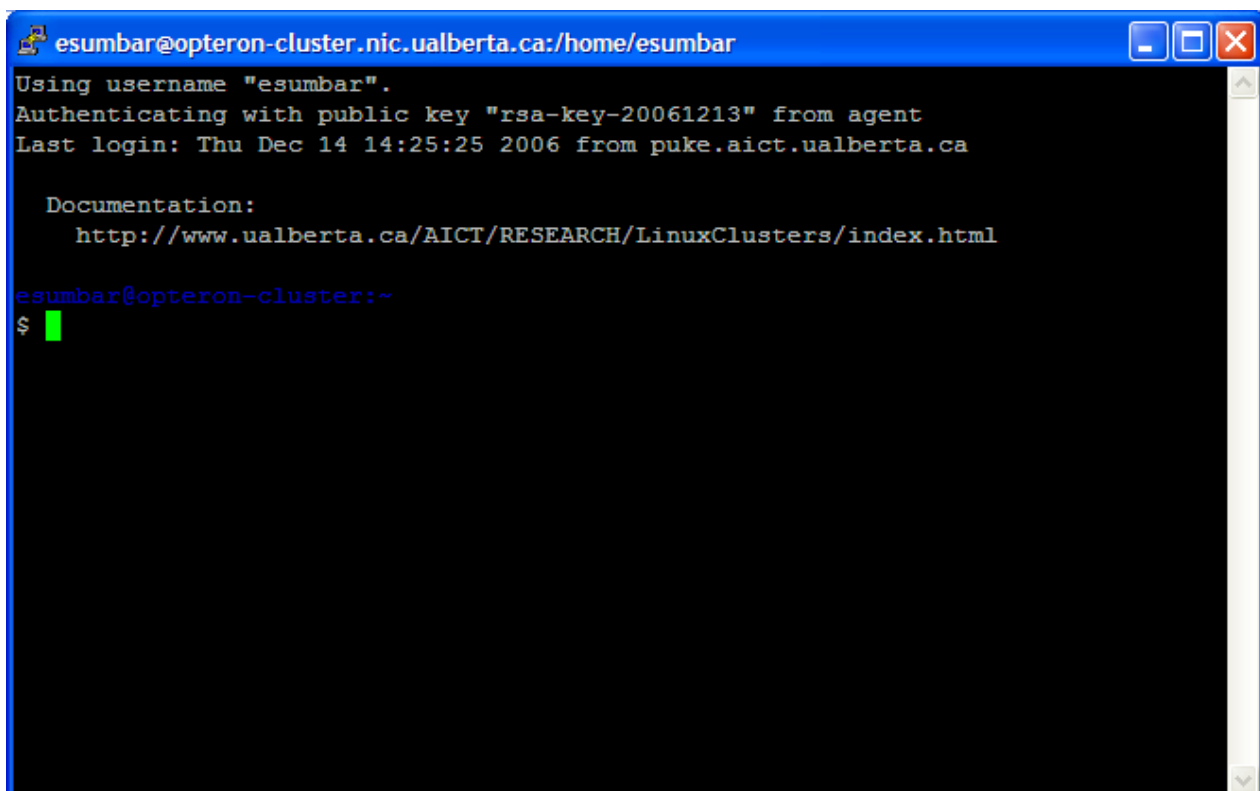


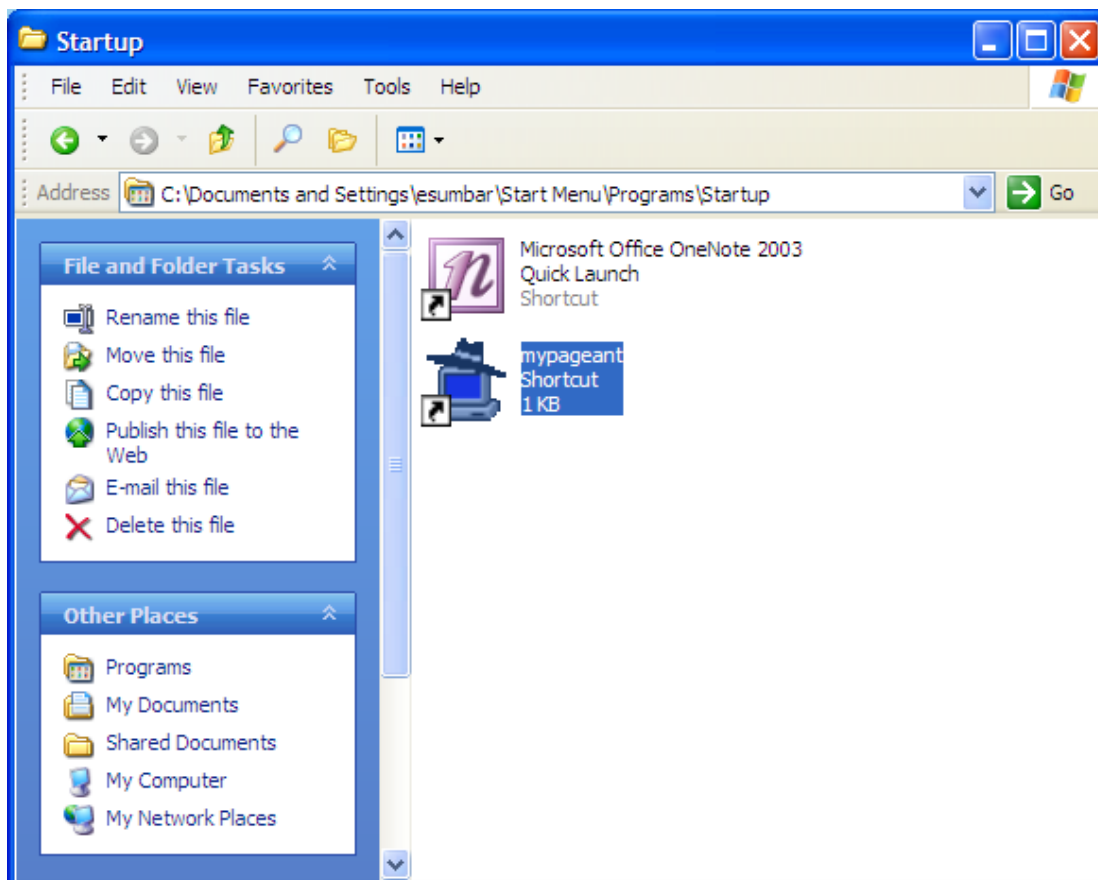
Fig. 11 Authentication handled by Pageant.

For convenience, you can have Pageant start up and load the key automatically whenever you log into your Windows desktop. Do this by creating a shortcut in your Startup folder as follows.

Go to the Startup folder by right-clicking the Start button, select Open, double-click on the Programs folder, then double-click on the Startup folder. Inside the Startup folder, right-click and select New > Shortcut. In the "Type the location of the item" text box, enter the full path to the Pageant program followed by the full path to the key file. For example,

```
"c:\program files\putty\pageant.exe" "c:\documents and settings\esumbar\pka-putty\mykey.ppk"
```

Click Next. Enter "mypageant" (or a name of your choice) in the "Type a name for this shortcut" box, then click Finish.

**Fig. 12** Starting Pageant automatically.

The next time you log in to Windows, Pageant will start automatically, load the specified key, and prompt you for the passphrase.

Security Considerations

In essence, the private key that you generate represents your "identity" in the public key authentication method. Therefore, as already stated, the private key should be stored in a file that only you can access, and the key should be encrypted with a passphrase for added security. If this is not possible, do not use public key authentication.

When using Pageant, the private-key file needs to be available only for the time it takes to add the key. As such, you can enhance security by storing the key on personal removeable media such as a USB memory stick. Make it available only when necessary. Insert the media before logging in to Windows, then remove it after answering the passphrase

prompt. When not in use, keep the removeable media in a safe place. Some USB memory sticks are designed as key fobs for example.

It is unwise to allow agent forwarding in the "Authentication parameters" box on the Connection > SSH > Auth window. If the remote host is insecure, the forwarded agent could potentially be used by unauthorized persons. Fortunately, this is off by default.

If you suspect that your private key has been compromised, immediately remove the associated public key from the `authorized_keys` file on all of your remote hosts or have the system administrators do it for you. Before generating a new key, identify the source of the compromise and adopt preventive measures to minimize your vulnerability in the future. If this is not possible, do not use public key authentication.

You can also limit the impact of a lost or stolen private key by restricting public key authentication to specified hosts. For example, prepending `from="*.ualberta.ca"` to a public key in the `authorized_keys` file on a remote host will permit computers only from the `ualberta.ca` domain to connect to this remote host with this public key. See the `AUTHORIZED_KEYS FILE FORMAT` section in `man sshd` on a Unix machine for additional details.

As an additional precaution, use your current private key for only a limited time, say six months to one year. Periodically delete it and purge all your remote `authorized_keys` files, then generate a new private key and distribute the new public key. However, juggling multiple private keys and numerous remote hosts can get complicated. Keep it simple by maintaining only one private key for public key authentication.

Finally, remember that your password is still valid and password authentication is still available. However, with public key authentication set up, you can "randomize" your password if you suspect it to be weak and then forget about it. If you ever need to use a password in the future, a system administrator can always reset it.

© 2006 University of Alberta