在 Win7 下使用 XShell 的 SSH Public key 連線遠端 Ubuntu 伺服器

1. 在 Ubuntu 16.04 環境安裝並啟動 SSH 服務：

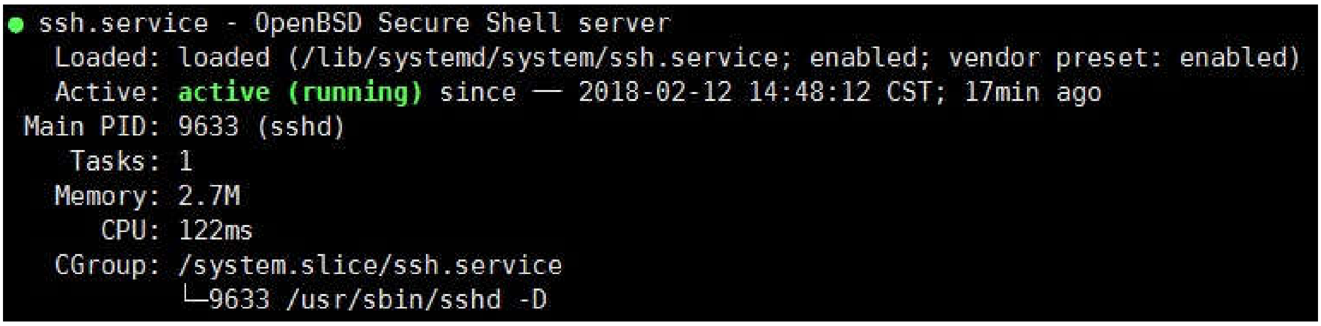
   在 Ubuntu 的主機上開啟終端視窗，並輸入下列指令：

```
$ sudo apt-get update
$ sudo apt-get upgrade
$ sudo apt-get install openssh-server
```

   安裝完畢後，重新啟動 SSH 服務並檢查是否正常，輸入下列指令：

```
$ sudo service ssh restart
$ sudo service ssh status
```

   如果出現綠色的 active 表示成功啟動，如圖 1：



```
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since — 2018-02-12 14:48:12 CST; 17min ago
 Main PID: 9633 (sshd)
    Tasks: 1
   Memory: 2.7M
      CPU: 122ms
   CGroup: /system.slice/ssh.service
           └─9633 /usr/sbin/sshd -D
```

圖 1 SSH 服務的狀態

2. 設定 Ubuntu 的防火牆：

   執行指令如下：

```
$ sudo ufw default deny incoming
$ sudo ufw default allow outgoing
$ sudo ufw allow ssh
$ sudo ufw enable
```

   其指令的意義分別是拒絕所有進入伺服器的請求，允許所有來開伺服器的請求，允許 SSH 服務的請求，和開機時啟動防火牆(Uncomplicated Firewall; ufw) 服務。
   如果要確認 ufw 是否正常啟用，可以以輸入下列指令：

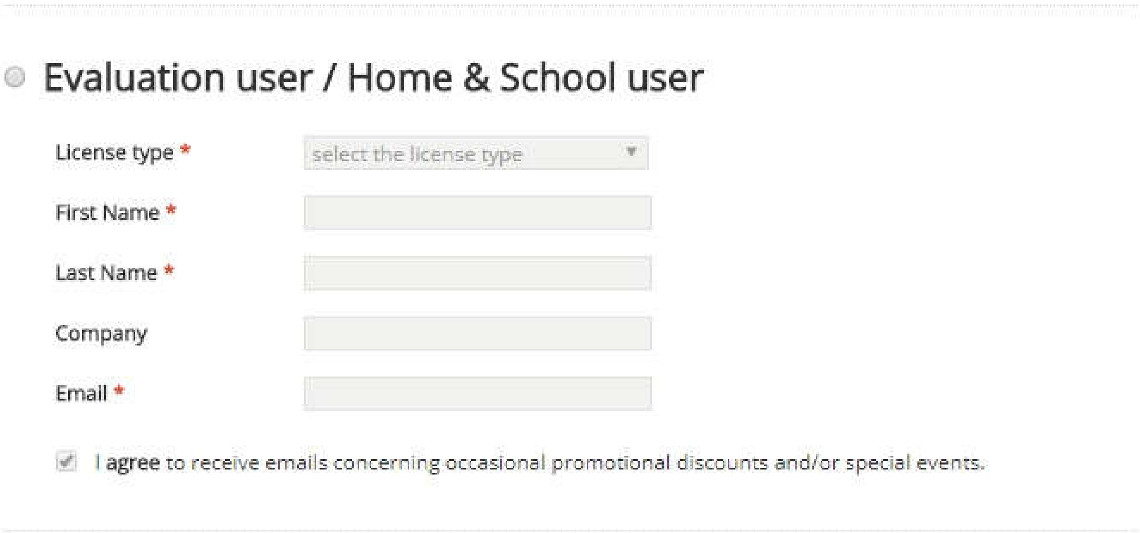
```
$ sudo service ufw status
```

出現綠色的 active 就是正常啟動了。如果想要知道現在開放了哪些服務或連接埠 (port)，則輸入下列指令：

```
$ sudo ufw status
```

3. 在 Windows 7 環境下載和安裝 XShell 軟體：

官網網址：https://www.netsarang.com/download/down_form.html?code=522
下載頁面如圖 2，填寫基本資料後，官網會把下載連結寄到登記的 email 信箱，點擊連結即可下載。



○ Evaluation user / Home & School user

License type * select the license type ▾

First Name *

Last Name *

Company

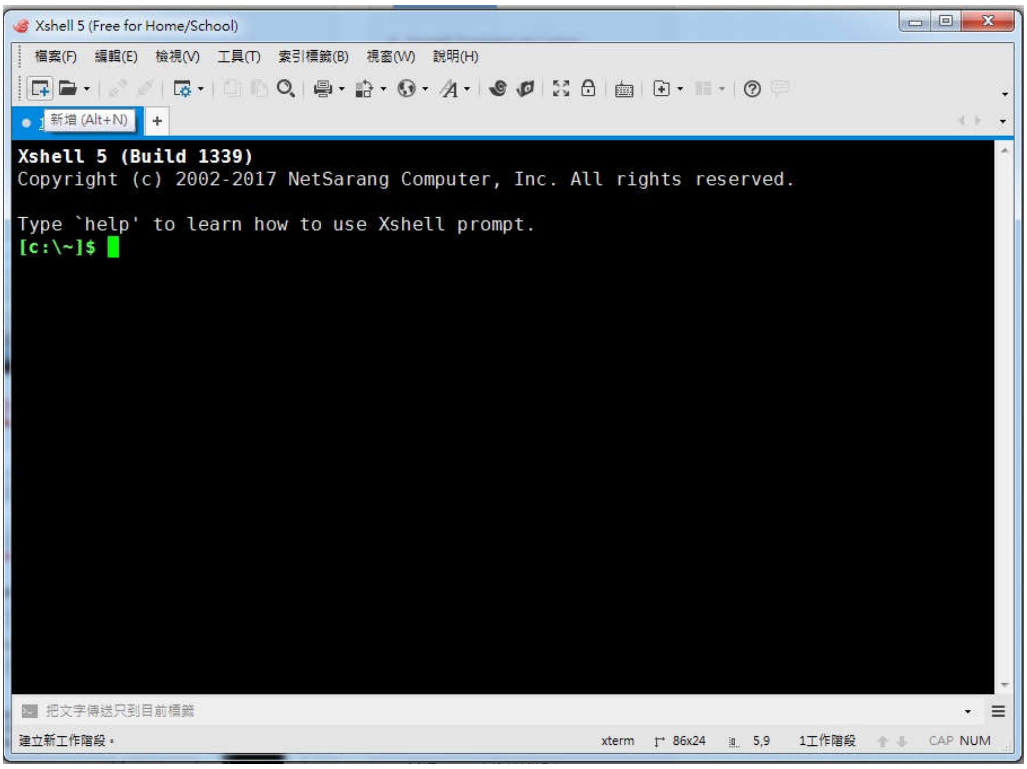
Email *

☑ I agree to receive emails concerning occasional promotional discounts and/or special events.

圖 2 下載 XShell 軟體

下載後立即安裝 XShell，安裝後桌面會有圖示，如圖 3。點擊後即可開啟 XShell。開啟畫面如圖 4。

圖 3 XShell 圖示


Xshell 5 (Free for Home/School)
檔案(F) 編輯(E) 檢視(V) 工具(T) 索引標籤(B) 視窗(W) 說明(H)
新增 (Alt+N)
把文字傳送只到目前標籤
建立新工作階段。
xterm
86x24
5,9
1工作階段
CAP NUM

```
Xshell 5 (Build 1339)
Copyright (c) 2002-2017 NetSarang Computer, Inc. All rights reserved.

Type `help' to learn how to use Xshell prompt.
[c:\~]$
```

圖 4 XShell 畫面

4. 在 XShell 下產生 Public key：
   執行程序如附件一。

5. 將 XShell 產生的 Public key 加到 Ubuntu 上：

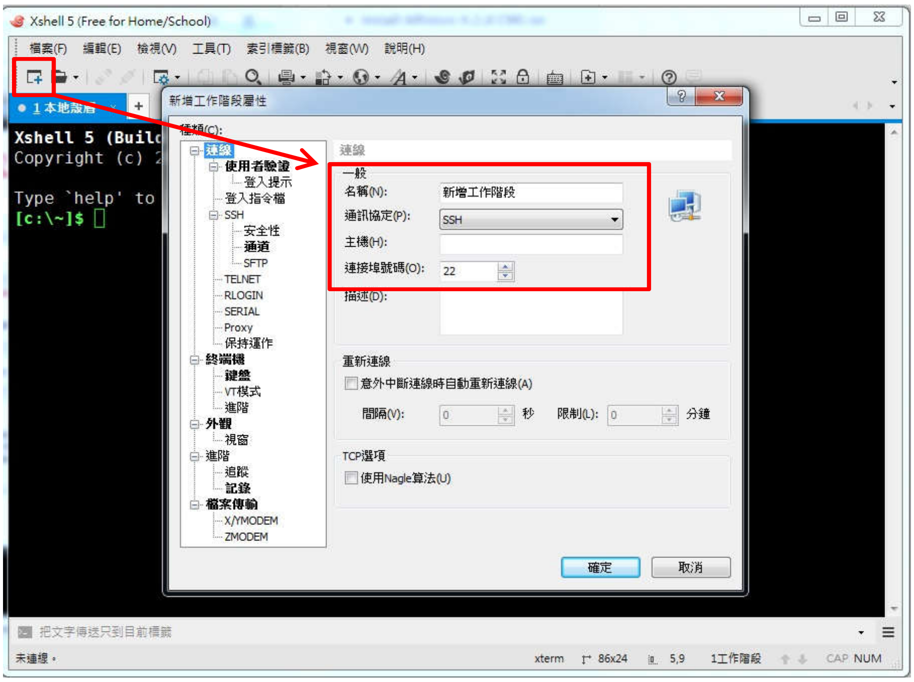
   (1). 在 XShell 建立新的連線設定，如圖 5。輸入名稱、主機 IP 後按確定。
   (2). 第一次連線仍需要使用 SSH 連線，等這次設定好 SSH public key 連線後，以後才可以使用 SSH public key 連線。
   (3). 使用剛剛建立的連線連到 Ubuntu。
   (4). 修改 /etc/ssh/sshd_config 檔案，啟動 AuthorizedKeysFile，執行程序如下：

```
$ sudo nano /etc/ssh/sshd_config
```

找到圖 6 紅框部分，移除 ‘#’。接下來編輯 ~/.ssh/authorized_keys，執行下列指程序：

```
$ sudo ~/.ssh/authorized_keys
```

將剛剛在 SSH 產生的 public key 的內容貼到 ~/.ssh/authorized_keys 檔案中，如圖 7。



```
Xshell 5 (Build
Copyright (c) 2

Type `help' to
[c:\~]$
```

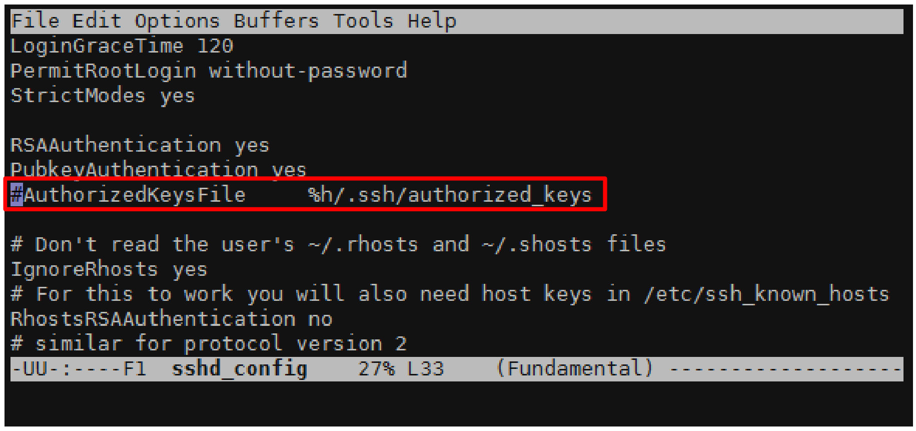
連線

一般
名稱(N): 新增工作階段
通訊協定(P): SSH
主機(H):
連接埠號碼(O): 22
描述(D):

重新連線
□ 意外中斷連線時自動重新連線(A)
間隔(V): 0 秒 限制(L): 0 分鐘

TCP選項
□ 使用Nagle算法(U)

圖 5 建立新的 XShell 連線

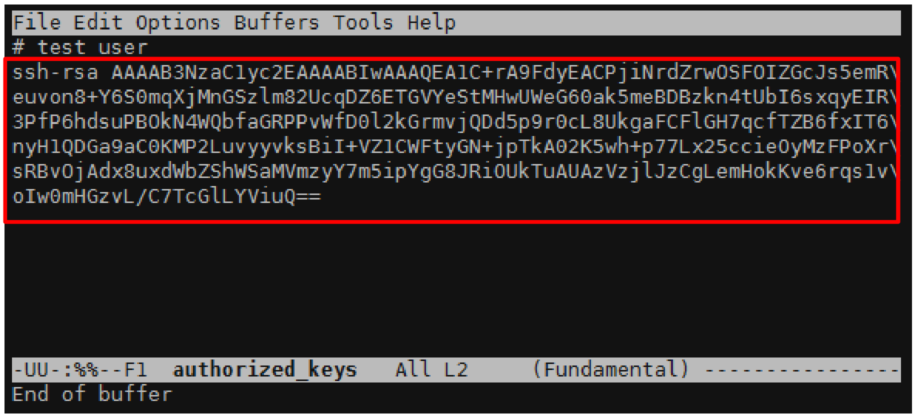


```
File Edit Options Buffers Tools Help
LoginGraceTime 120
PermitRootLogin without-password
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile     %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
-UU-:----F1  sshd_config     27% L33    (Fundamental) ------------------
```

圖 6 AuthorizedKeysFile



```
File Edit Options Buffers Tools Help
# test user
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA1C+rA9FdyEACPjiNrdZrwOSFOIZGcJs5emR\
euvon8+Y6S0mqXjMnGSzlm82UcqDZ6ETGVYeStMHwUWeG60ak5meBDBzkn4tUbI6sxqyEIR\
3PfP6hdsuPBOkN4WQbfaGRPPvWfD0l2kGrmvjQDd5p9r0cL8UkgaFCFlGH7qcfTZB6fxIT6\
nyH1QDGa9aC0KMP2LuvyyvksBiI+VZ1CWFtyGN+jpTkA02K5wh+p77Lx25ccieOyMzFPoXr\
sRBvOjAdx8uxdWbZShWSaMVmzyY7m5ipYgG8JRiOUkTuAUAzVzjlJzCgLemHokKve6rqslv\
oIw0mHGzvL/C7TcGlLYViuQ==




-UU-:%%--F1  authorized_keys    All L2     (Fundamental) ---------------
End of buffer
```

圖 7 ~/.ssh/authorized_keys

6. 修改 authorized_keys 的檔案屬性及擁有者，並重新啟動 SSH 服務：

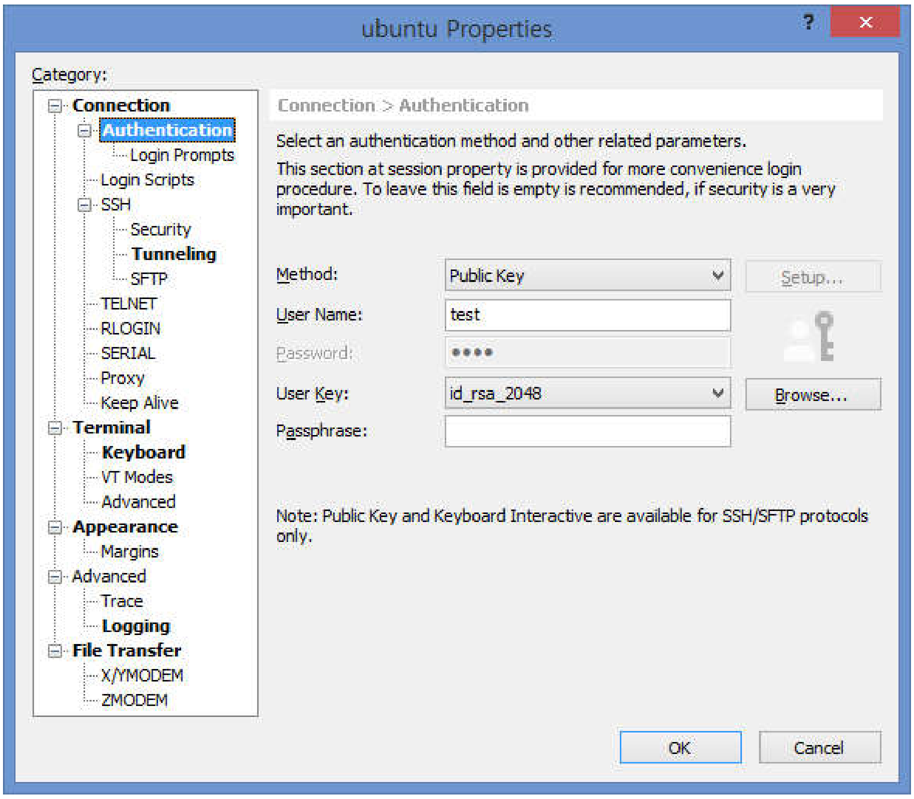
請執行下列程序：

```
$ sudo chmod 600 ~/.ssh/authorized_keys
$ sudo chown [user name]:[user group] ~/.ssh/authorized_keys
$ sudo service ssh restart
```

其中的 user name 和 user group 是在建立 XShell 連線設定時設定的帳號，也是登入 Ubuntu 後的帳號，所以必須是已經在 Ubuntu 裡已經建好的帳號，而且需要有 sudo 權限。

7. 使用 XShell 測試 ssh public key

將在 XShell 建立的連線設定的方法改為 Public Key，如圖 8，按下 ok 後就可以連線進入 Ubuntu 了。



Select an authentication method and other related parameters.

This section at session property is provided for more convenience login procedure. To leave this field is empty is recommended, if security is a very important.

Method: Public Key

User Name: test

Password: ●●●●

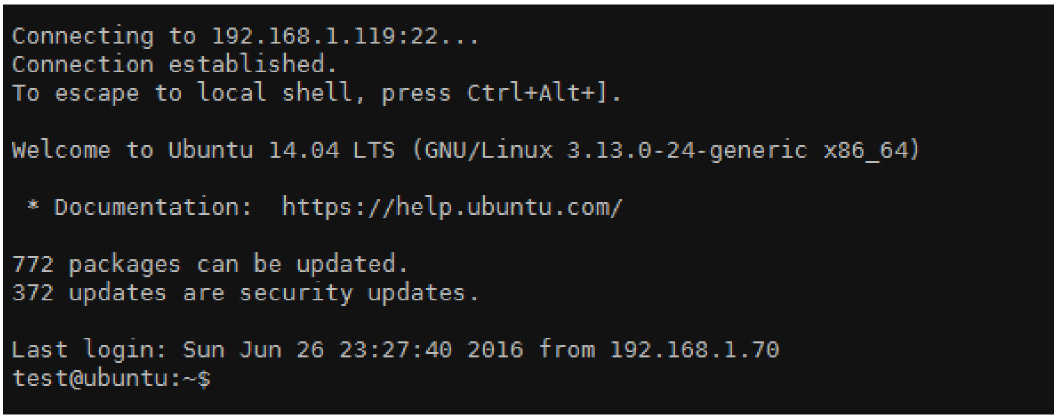
User Key: id_rsa_2048

Passphrase:

Note: Public Key and Keyboard Interactive are available for SSH/SFTP protocols only.

圖 8 使用 Public key 方法連接 Ubuntu

連線成功後的畫面如圖 9。



```
Connecting to 192.168.1.119:22...
Connection established.
To escape to local shell, press Ctrl+Alt+].

Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

772 packages can be updated.
372 updates are security updates.

Last login: Sun Jun 26 23:27:40 2016 from 192.168.1.70
test@ubuntu:~$
```

圖 9 連線成功

附件一：

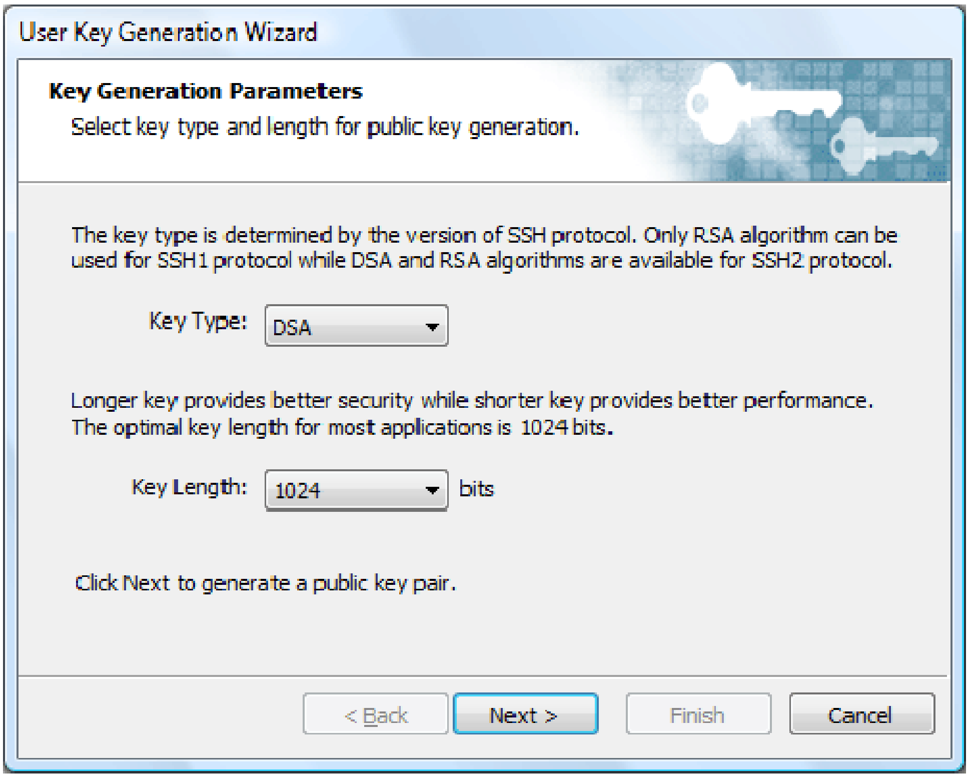
資料來源：https://www.netsarang.com/tutorial/xshell/1005/title

Public Key User Authentication

Last modified: Thursday, October 29, 2009 12:29 AM
Xshell supports the public key user authentication method which is an alternative way of identifying the user to the remote server instead of typing the password.
To use the public key user authentication method, a user generates a key pair consisting of a public key (which everybody is allowed to know) and a private key (which conceal from the rest). Private key is used in the public key authentication process to generate signature and the public key is used by the server to verify the signature. In other words, private key works as an identification of a user. Also, the user should register his public key to the server for getting authenticated.

Generating a key pair

1. the Tools menu, click User Key Manager.
2. Click Generate button to open User Key Generation Wizard.



User Key Generation Wizard

Key Generation Parameters
Select key type and length for public key generation.

The key type is determined by the version of SSH protocol. Only RSA algorithm can be used for SSH1 protocol while DSA and RSA algorithms are available for SSH2 protocol.

Key Type: DSA

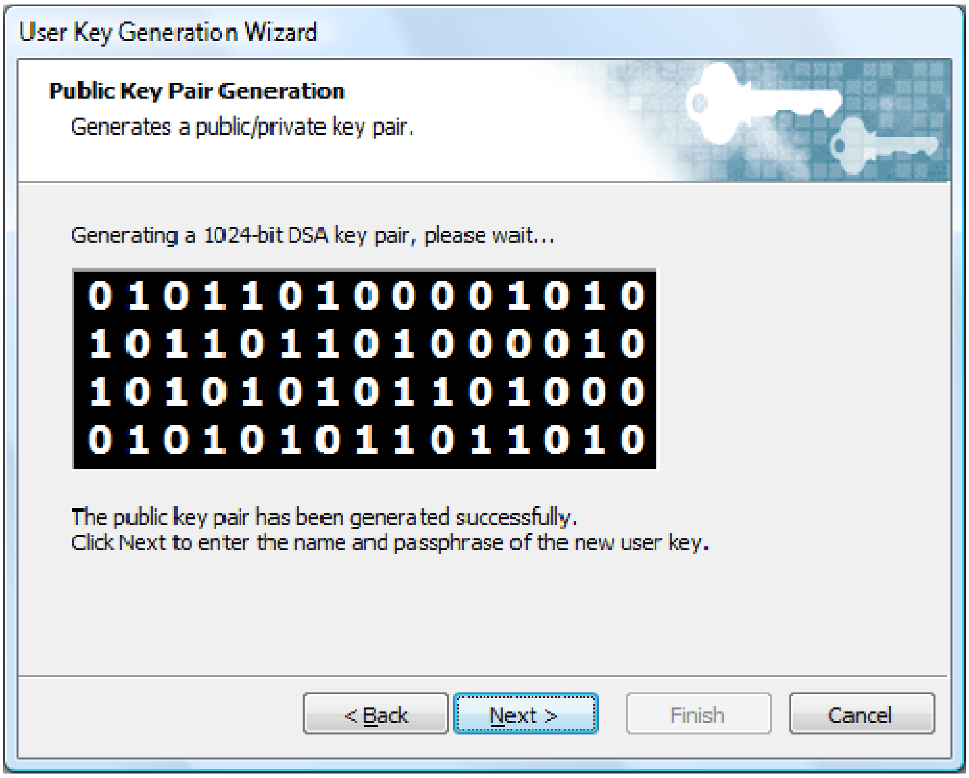
Longer key provides better security while shorter key provides better performance. The optimal key length for most applications is 1024 bits.

Key Length: 1024 bits

Click Next to generate a public key pair.

3. the Key Type list, select a proper key type. For the SSH1 protocol, only RSA algorithm is supported. So, select the RSA. For the SSH2 protocol, more than one type of algorithm is supported. Xshell supports both RSA and DSA.

4. In the Key Length box, type or select a key length. Longer keys provide better security and shorter keys provide better speed. The optimal key length for most applications is 1024 bits.
5. Click Next to proceed to the key generation step and wait until the key generation process completes. After the key generation process, click Next to enter the user key information.



User Key Generation Wizard

Public Key Pair Generation

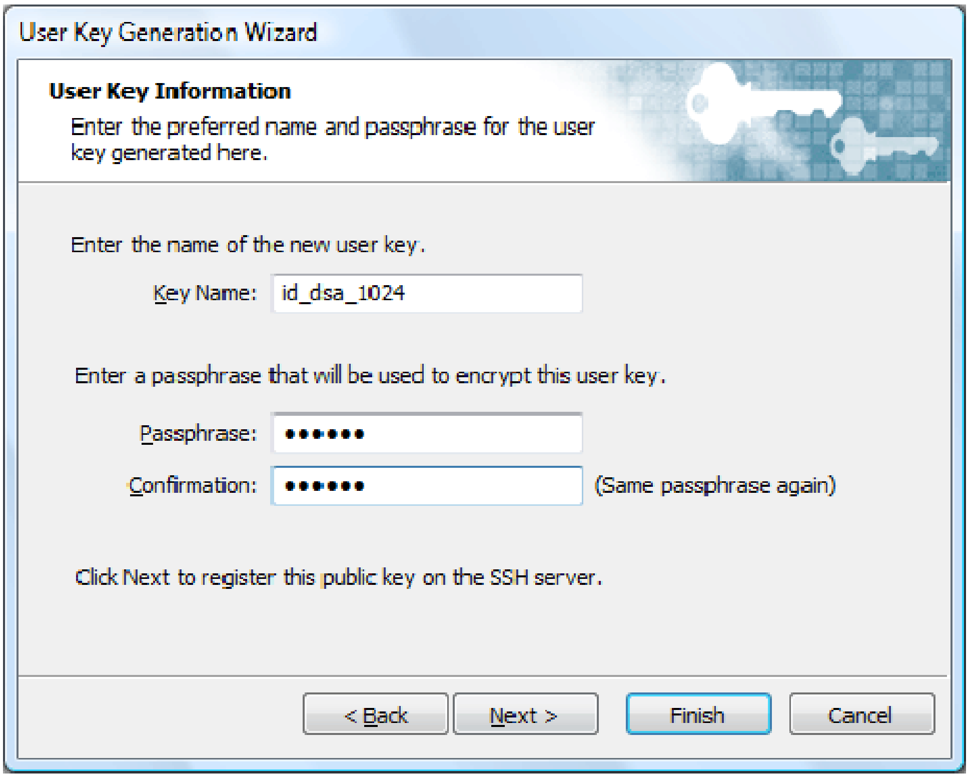
Generates a public/private key pair.

Generating a 1024-bit DSA key pair, please wait...

```
0 1 0 1 1 0 1 0 0 0 0 1 0 1 0
1 0 1 1 0 1 1 0 1 0 0 0 0 1 0
1 0 1 0 1 0 1 0 1 1 0 1 0 0 0
0 1 0 1 0 1 0 1 1 0 1 1 0 1 0
```

The public key pair has been generated successfully.
Click Next to enter the name and passphrase of the new user key.

6. In the Key Name box, type a key name.



User Key Generation Wizard

User Key Information

Enter the preferred name and passphrase for the user key generated here.

Enter the name of the new user key.

Key Name: id_dsa_1024

Enter a passphrase that will be used to encrypt this user key.

Passphrase: ••••••

Confirmation: •••••• (Same passphrase again)

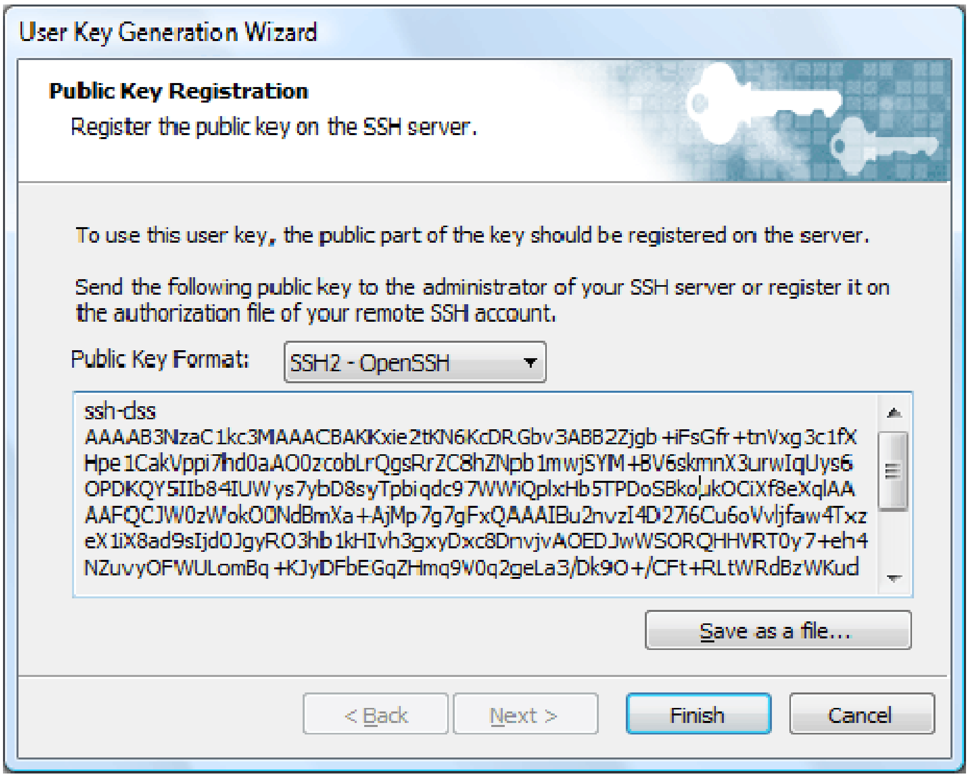
Click Next to register this public key on the SSH server.

7. In the Passphrase box, type a passphrase. The passphrase is used in encrypting a private key file.
8. In the Confirmation box, type the same passphrase you typed in the Passphrase box to confirm your input.
9. Click Next to register the public key to the server.

Now, all key generation steps are finished, but you must configure the server to accept your public key for authentication. To configure the server, see the following Registering a public key on the server section.

Registering a public key on the server

To put the key pair you have generated in the Generating a key pair section in use, you have to register the public key on your remote account so that the server can authenticate the user with it. Registering a public key varies with the version of SSH protocol and the vendor of SSH server.



Public Key Registration

Register the public key on the SSH server.

To use this user key, the public part of the key should be registered on the server.

Send the following public key to the administrator of your SSH server or register it on the authorization file of your remote SSH account.

Public Key Format: SSH2 - OpenSSH

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAKKxie2tKN6KcDRGbv3ABB2Zjgb+iFsGfr+tnVxg3c1fX
Hpe1CakVppi7hd0aAO0zcobLrQgsRrZC8hZNpb1mwjSYM+BV6skmnX3urwIqUys6
OPDKQY5IIb84IUWys7ybD8syTpbiqdc97WWiQplxHb5TPDoSBkoJkOCiXf8eXqlAA
AAFQCJW0zWokO0NdBmXa+AjMp7g7gFxQAAAIBu2nvzI4D27i6Cu6oVvljfaw4Txz
eX1iX8ad9sIjd0JgyRO3hb1kHIvh3gxyDxc8DnvjvAOEDJwWSORQHHVRT0y7+eh4
NZuvyOFWULomBq+KJyDFbEGqZHmq9V0q2geLa3/Dk9O+/CFt+RLtWRdBzWKud
```

- SSH1 protocol: Select SSH1 in the Public Key Format list and copy the public key into the file $HOME/.ssh/authorized_keys. (Note: You need to create this file if it does not exist.)
- OpenSSH server using SSH2: Select SSH2 - OpenSSH in the Public Key Format list, and copy the public key into the file $HOME/.ssh/authorized_keys2.
- ssh.com's SSH server using SSH2: Select SSH2 - IETF SECSH in the Public Key Format list and click Save as... to save the public key into a file. Then copy the public key file to the

directory $HOME/.ssh2/ and put the following line into the file $HOME/.ssh2/authorization:

Key mypublickey.pub

where mypublikey.pub is the public key file you have copied.

- For other SSH server products: Refer to the SSH server manual from its provider.

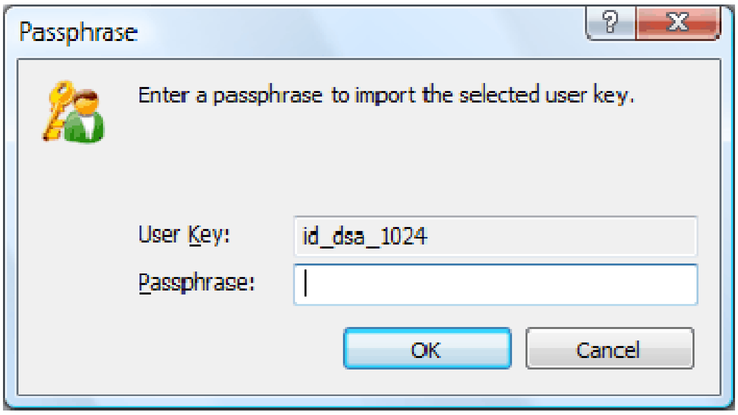
Now, you are ready for the public key authentication.

Importing a user key file

If you are already using the public key authentication somewhere else and want to reuse the private key with Xshell, you can import the private key. Currently, Xshell can read RSA private keys for the SSH1 protocol and OpenSSH's RSA/DSA keys for the SSH2 protocol along with Xshell's own user key files.

Follow the steps below to import user keys into Xshell's User Key Manager:

1. On the Tools menu, click User Key Manager.
2. Click Import... button to choose the user key file which will be imported.
3. After choosing the user key file, Passphrase dialog box will show up. (Only if the user key has passphrase setup.)


Passphrase

Enter a passphrase to import the selected user key.

User Key: id_dsa_1024

Passphrase:

4. In the Passphrase box, enter the passphrase of the user key.
5. Click OK.