Quick Note 10

SSH Access using RSA Key Authentication

Digi Technical Support

February 2016

Contents

Figures

1 VERSION

Version Number	Status
1.0	Published
2.0	Rebranded and updated with Pageant setup
2.1	Updated for new web GUI
2.2	Updated screenshots and instructions for new web interface, rebranding (Feb 2016)

1.1 Corrections

Requests for corrections or amendments to this Quick Note are welcome and should be addressed to: tech.support@digi.com

Requests for new Quick Notes can be sent to the same address.

2 SCENARIO

In order to securely administer the TransPort, SSH should be used for CLI access instead of telnet. Security can be increased further by using an RSA key pair to handle the authentication of the connection. When using public and private keys, the regular user passwords configured on the router are not used, the client must have the private key configured within the SSH software that can be verified by the public key on the router.

3 CONFIGURING THE SSH SERVER

This process involves generating a private key on the TransPort then configuring the SSH to use the key for SSH connections.

3.1 Generate the SSH Private Key

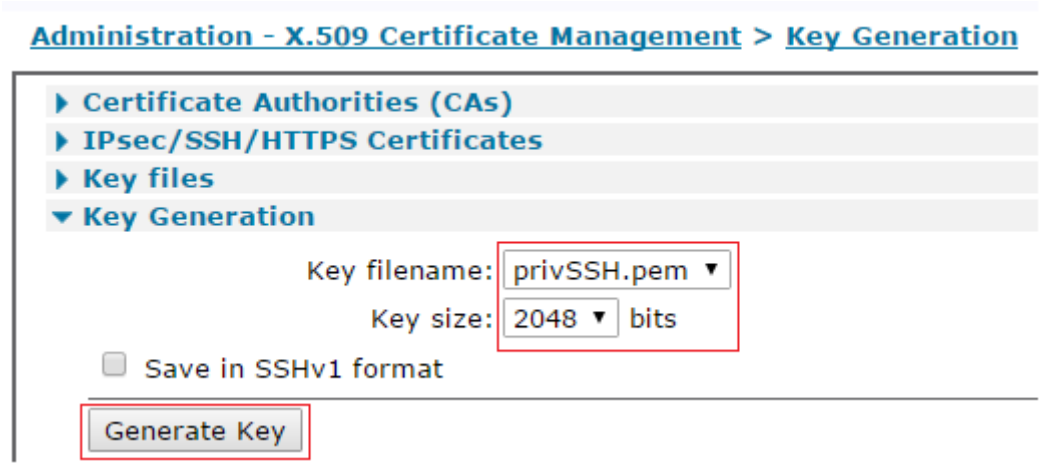

Figure 1: Generate the route SSH private key

From the "Key size" dropdown list, select a key size in bits. The larger the key, the more secure the connection, but also the larger the key, the slower the connection.

Click in the 'Key filename' dropdown box and start typing a name for the private key that will be generated.

Click on the "Generate Key" button to start the creation of the private key. After a few seconds, the browser will start updating with the progress of the key generation. When the key has been generated, the following information will be displayed.

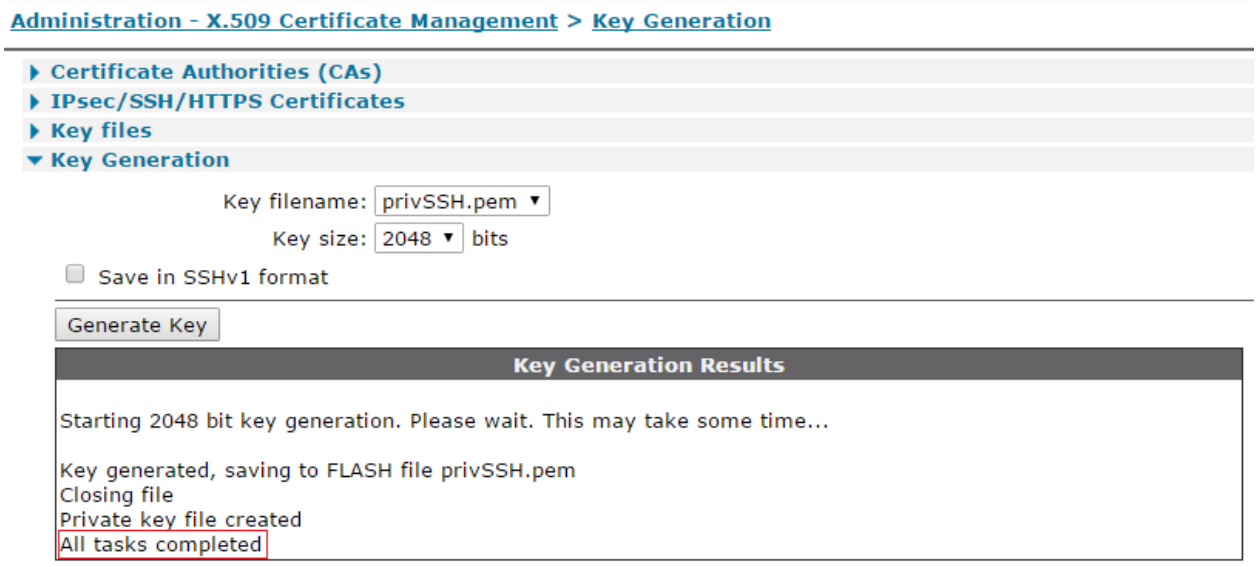

Figure 2: Successful key generation screen output

The private key has now been generated and saved to flash as privSSH.pem

3.2 Configure the SSH Server

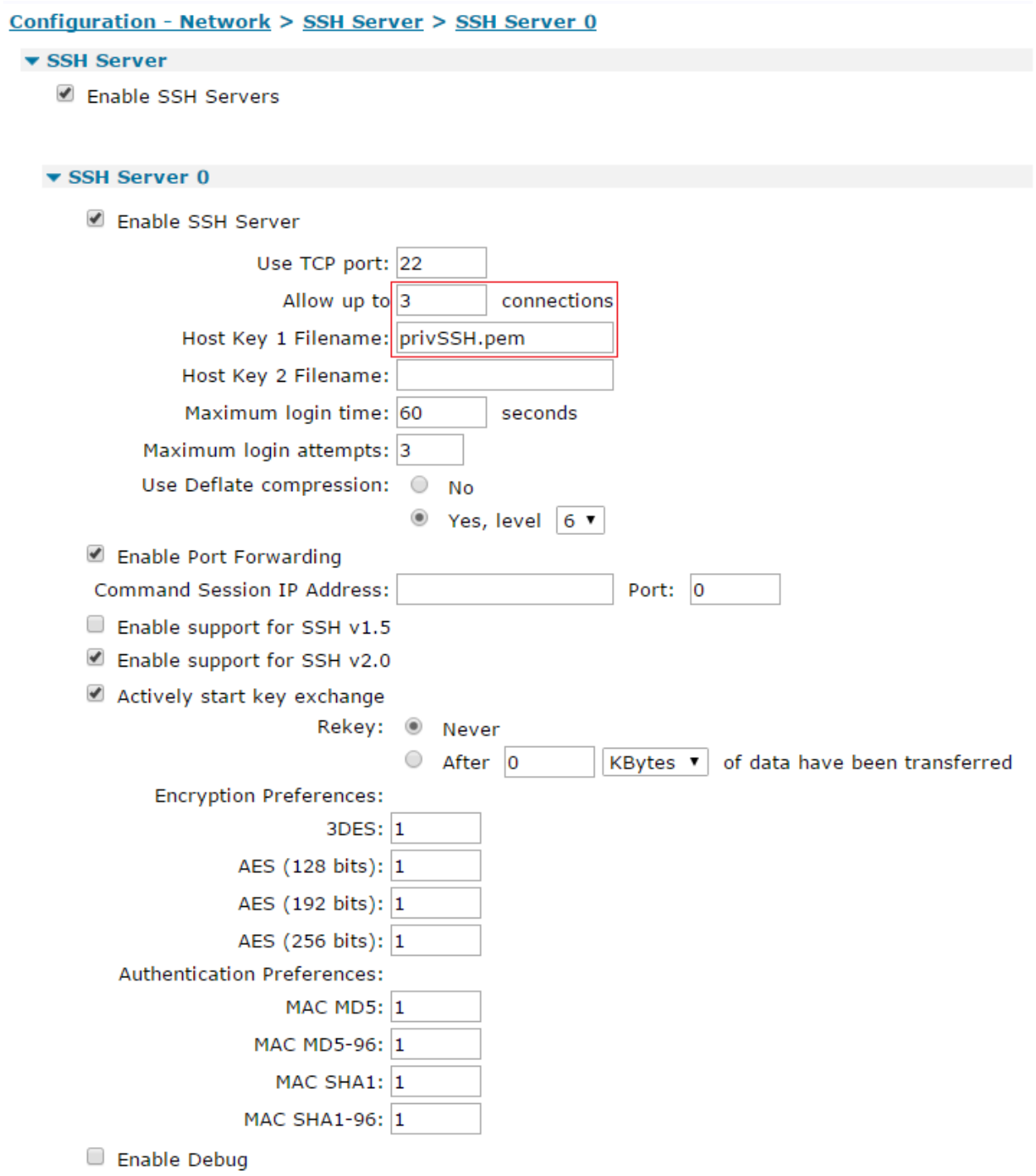

Figure 3: Setup the SSH o Server

Set the number of SSH servers to the number you will require into the "Allow up to *n* connections" field– for example if you want to be logged into the unit and do SFTP you will need at least 2 listening ports – if you wish to use Remote Manager over SSH to update and control the router then you may need up to 3 ports to allow for concurrent connections.

If the default values are correct, just enter the name of the private key generated in the previous step into the "Host key 1 filename" field.

Click the "**Apply**" button.

3.3 Test SSH Connectivity

A normal SSH connection to the router should now be possible without RSA authentication.

4 GENERATE THE KEY PAIR FOR RSA AUTHENTICATION

Download a copy of PuTTYgen. This will be used to create the public and private keys.

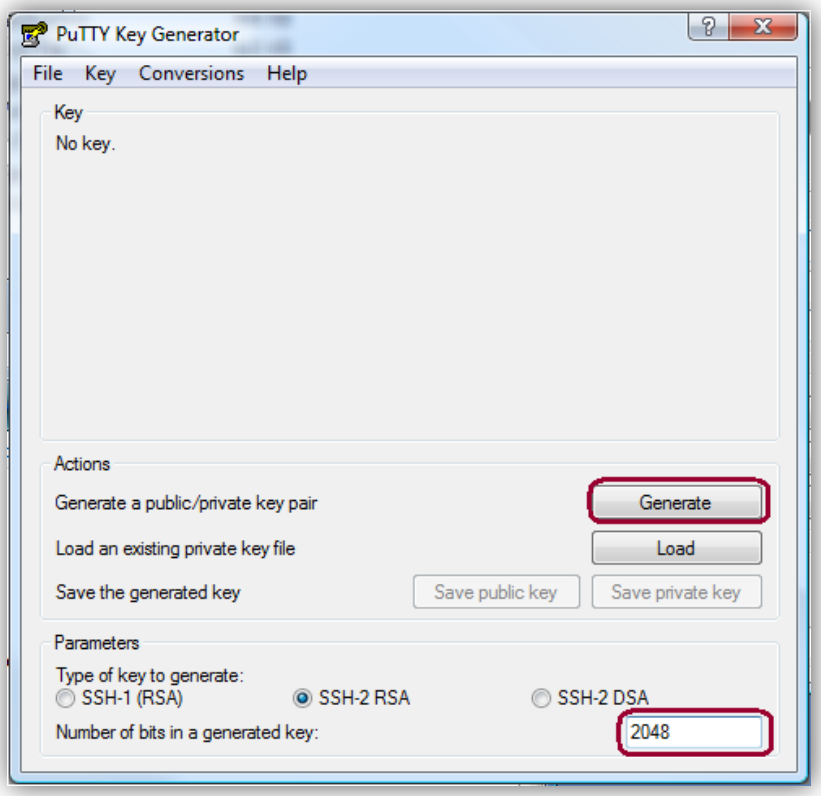

Figure 4: PuTTYgen Initiate key generation

Click on Generate to start the key generation process.

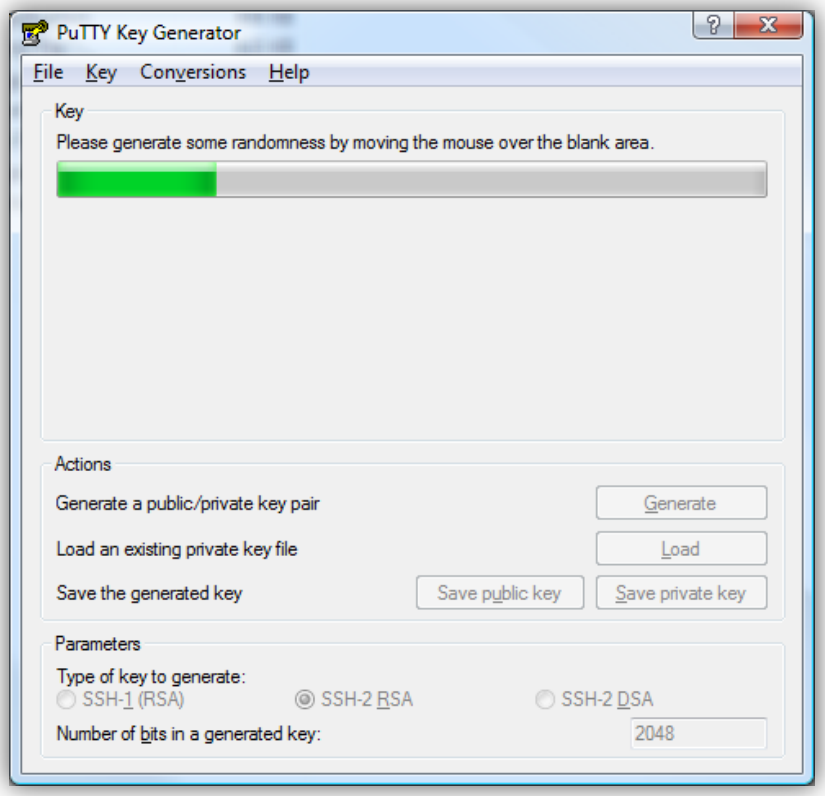

Figure 5: PuTTYgen Key Generation progress

Move the mouse pointer around below the white bar to generate randomness and the bar will fill up with green blocks.

When the process is complete, the following screen will be shown:

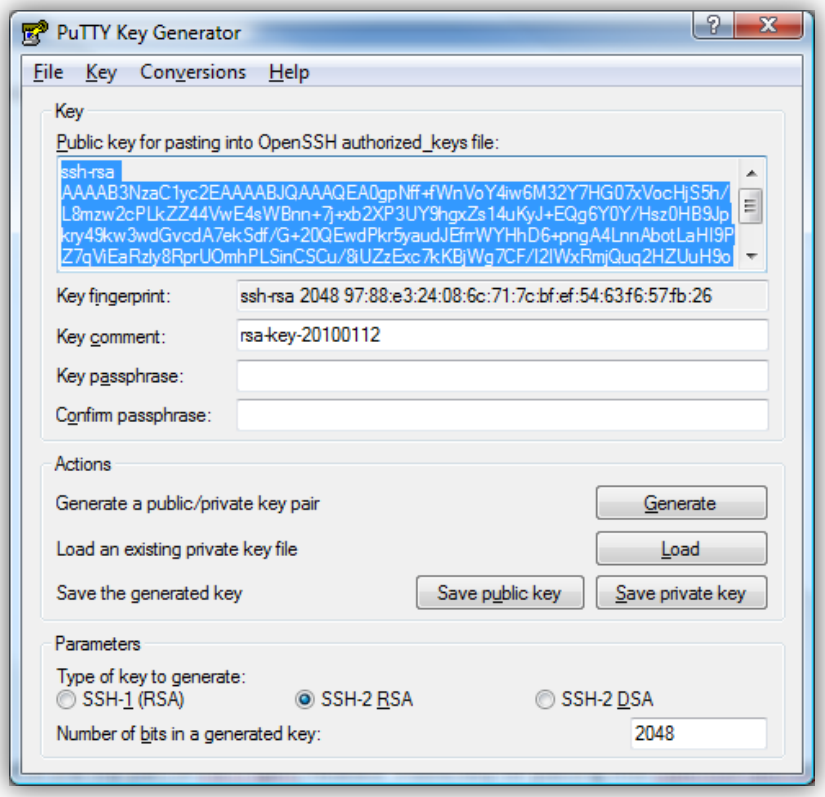

Figure 6: PuTTYGen copy generated public key

Copy the text in the top part of PuTTYgen, headed "Public key for pasting into OpenSSH authorized_keys file" to the clipboard. You can choose to enter a passphrase here, which you will be prompted for every time you load up the key. This adds some security, but if you are going to use this for automation you may not want to do this. It is optional to add a passphrase.

Open Notepad, paste the text from the clipboard, and then save the document as public.pem

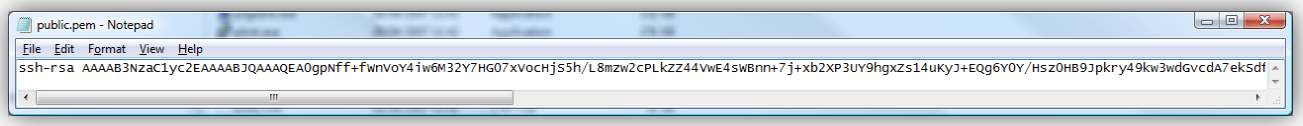

Figure 7: Save public SSH key

Notice that the pasted text is on 1 line only.

The file public.pem should now be transferred onto the TransPort using FTP.

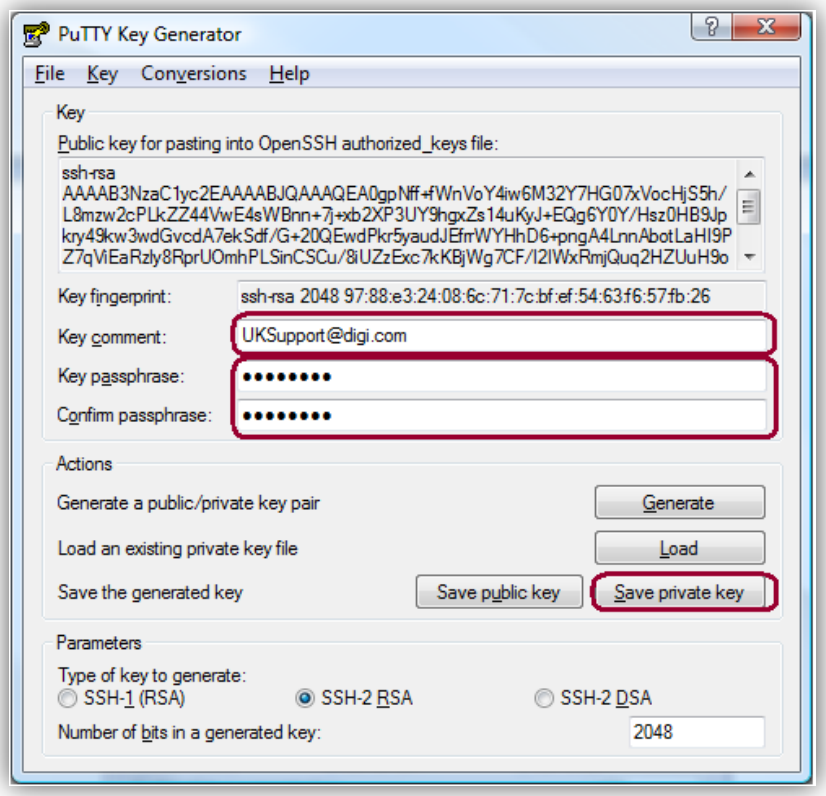

Figure 8: PuTTYgen set password and key comment then save private key

Enter a key passphrase and confirm it in the "Key passphrase" and "Confirm passphrase" fields. Change the "Key comment" to something that will identify the key if you use a tool like Pageant to manage your keys. Then click the "**Save private key**" button. Save it with the name "private.ppk"

4.1 Configure a User with the Public Key File

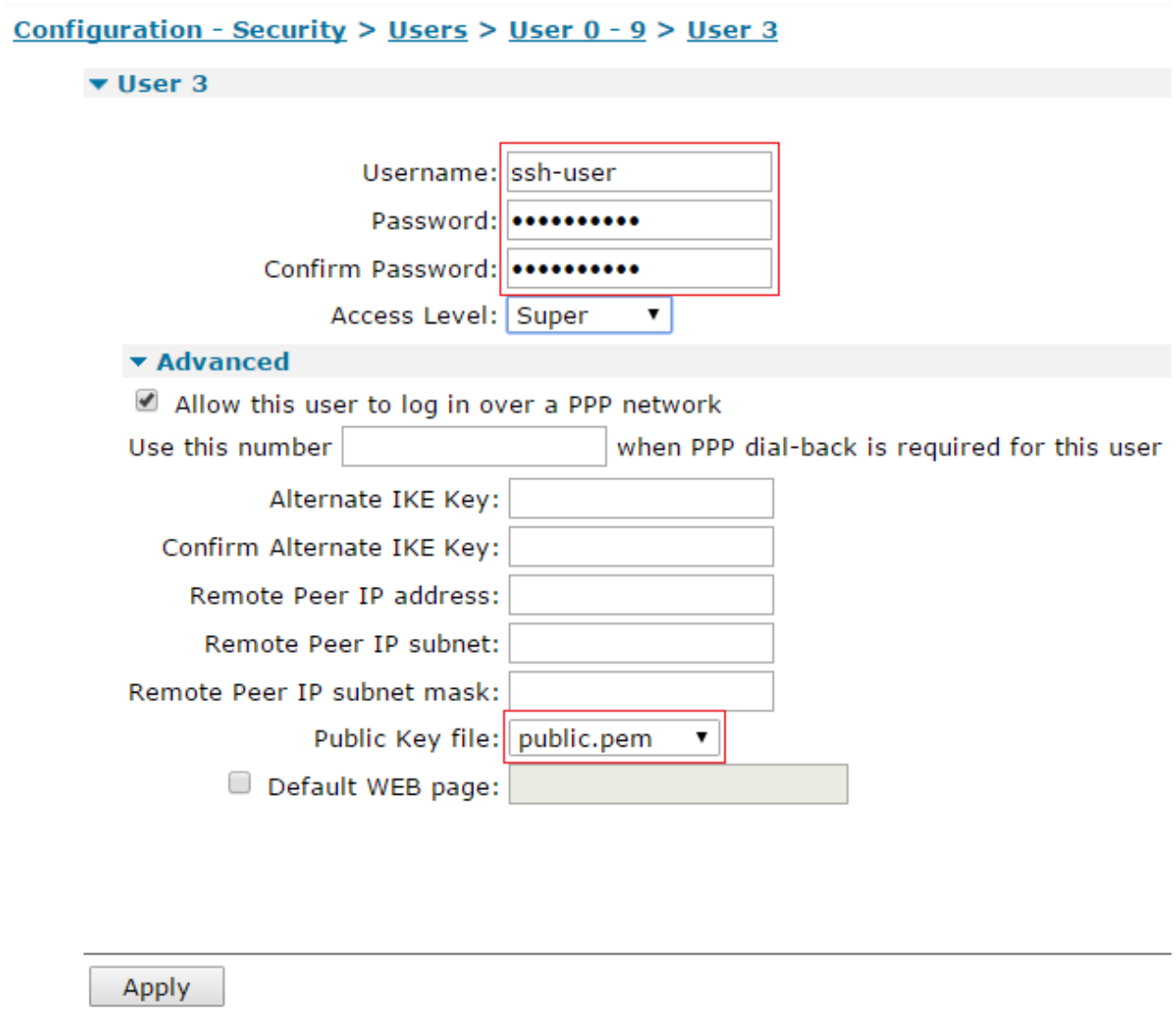

Figure 9: Setup remote access user to use SSH key authentication

Enter a name for the user in the "Username" field.

Enter a random, non-dictionary based password into the password fields. This password will not be used, but should the RSA authentication fail, the user will be displayed a password prompt. This password should be kept secret and not given to the user.

Select the public key from the dropdown list (the one that was created and FTP'd onto the router in the previous steps).

Click the "**Apply**" button.

4.2 Configure the SSH Client Software

The SSH client software (e.g. PuTTY) will need to be configured to use the private key generated in the previous steps.

In PuTTY expand **Connection > SSH > Auth** and enter the location of the private key file in the field titled "Private key file for authentication":

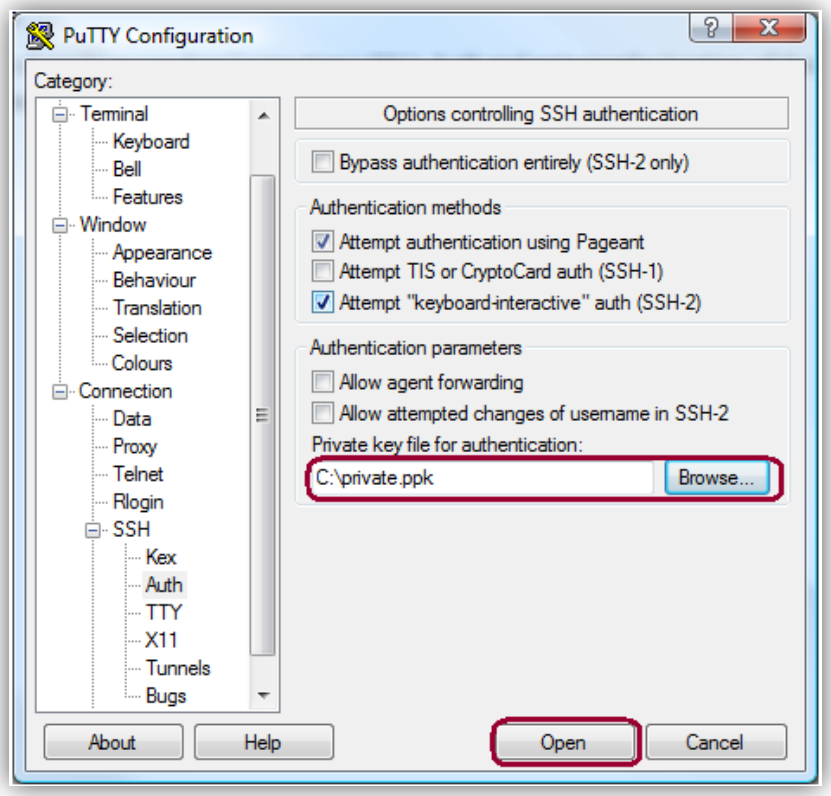

Figure 10: Setup Putty to use SSH key authentication

Save the username used to connect in **Connection > Data** into the field "Auto-login username":

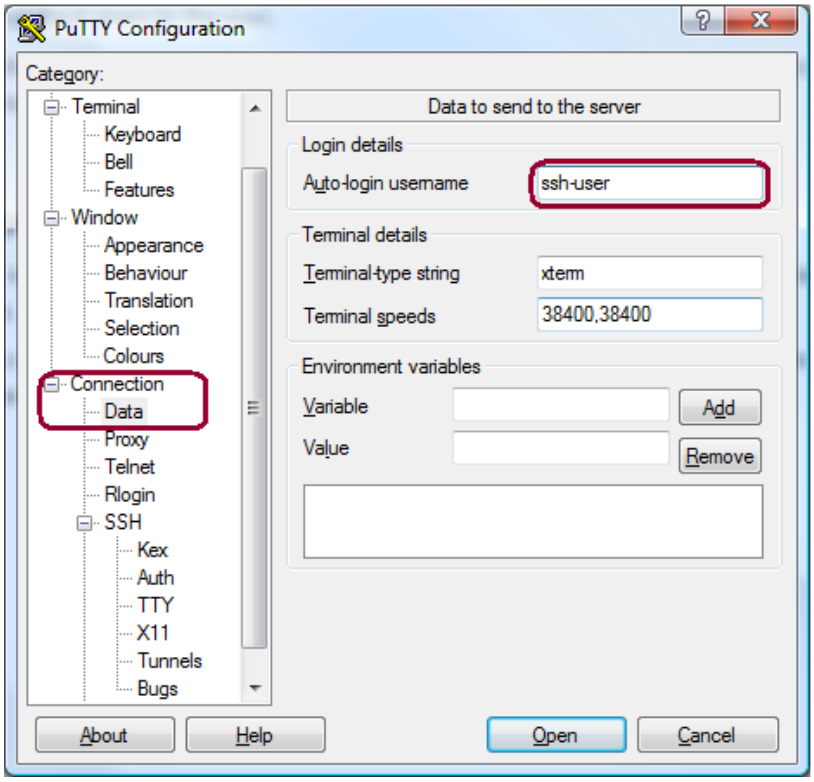

Figure 11: Setup PuTTY to auto use username

Return to the **Session** PuTTY connection tab and enter the IP or host name of the router into "Host Name (or IP Address)" and give the session a memorable name in the "Saved Sessions" field and then click the "**Save**" button:

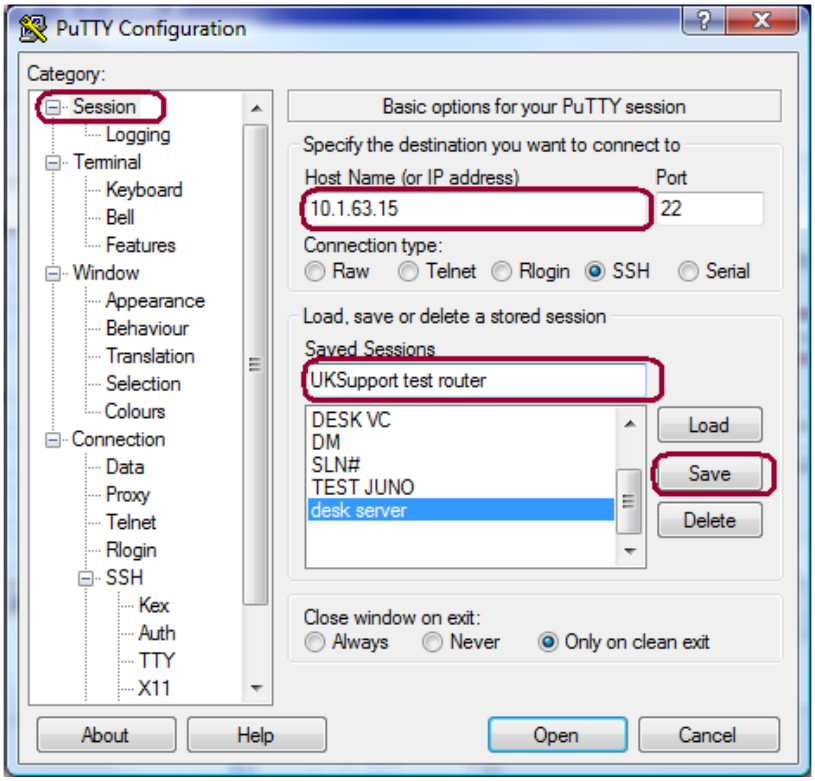

Figure 12: Save the PuTTY session

Your session should now be seen in the Saved Sessions list:

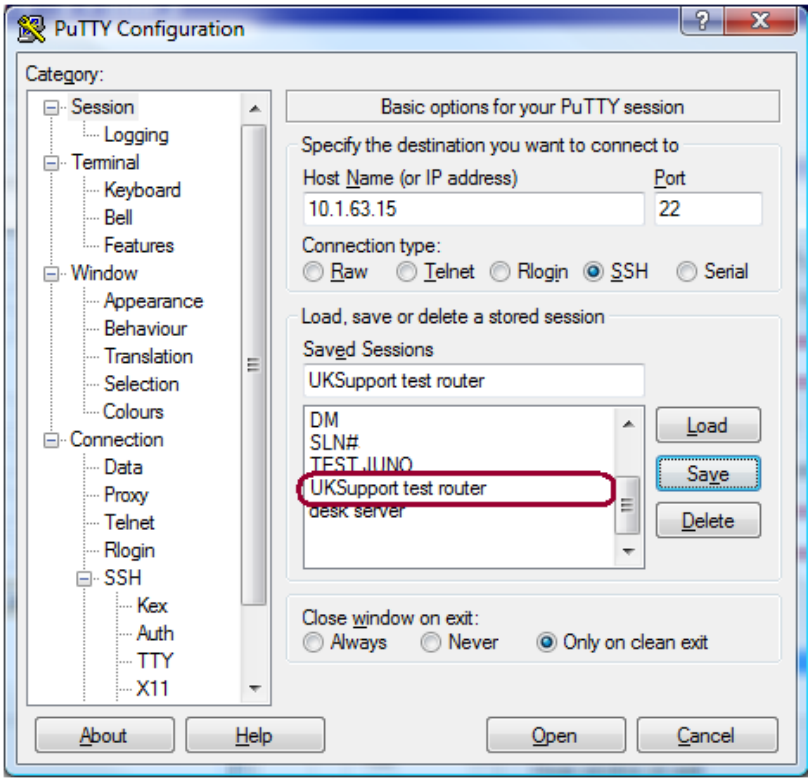

Figure 13: PuTTY displaying saved session

4.3 Using Pageant

Download Pageant (if you have installed the PuTTY suite of tools, this will be installed by default). To load your private key without further configuring PuTTY to use it, you can use Pageant to load the key up and this will be tried for all connections. You can load up a key automatically using this command:

" C:\Program Files\PUTT\Pageant.exe" " C:\private.ppk"

Enter the passphrase when prompted, if you have set one:

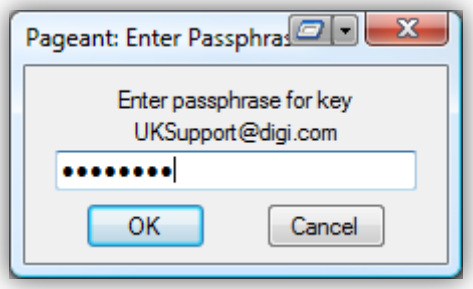

Figure 14: Pageant load key and enter passphrase

If you do not use the above command then you can load a key by right clicking on the Pageant, selecting "Add Key" then select key with the File Browser and then clicking "Open".

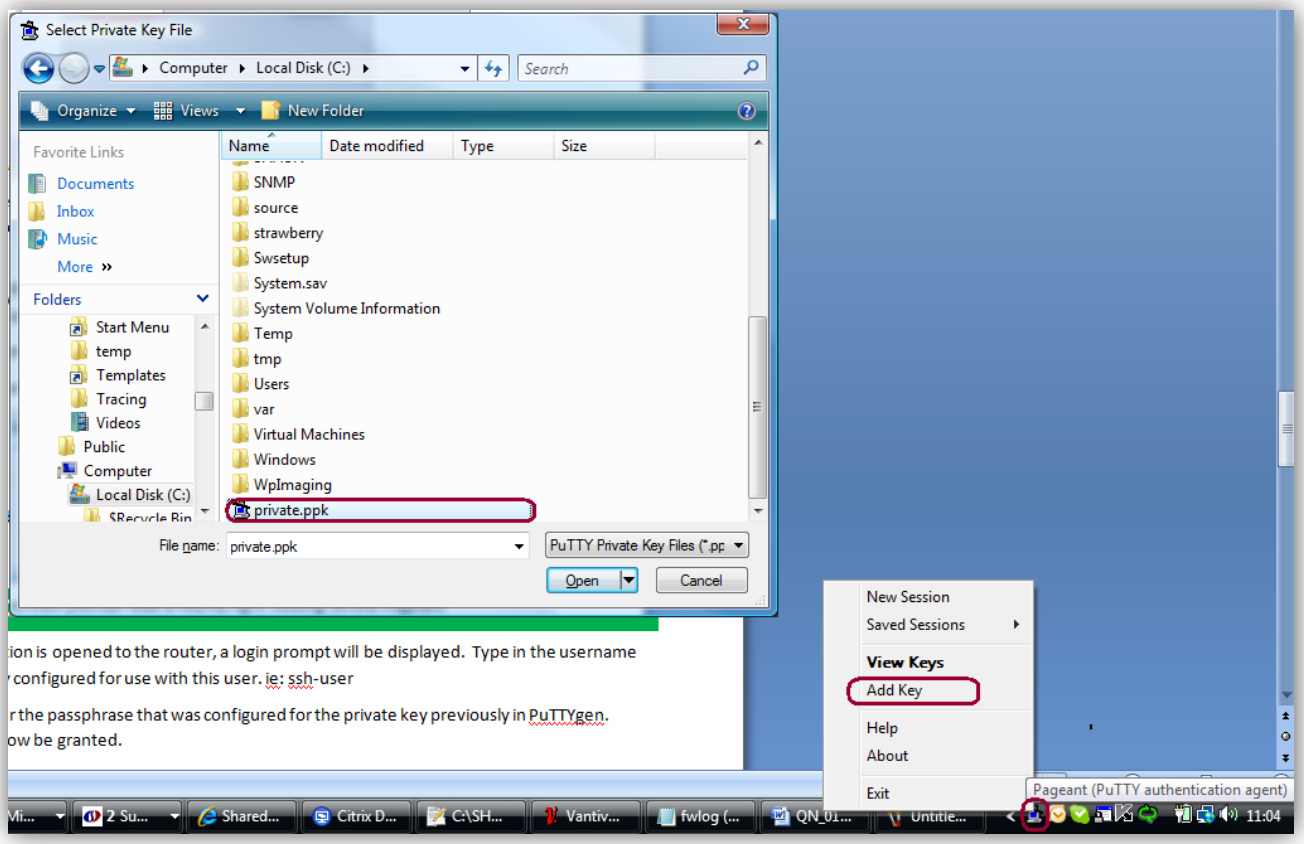

Figure 15: Manually loading the private key into Pageant

You will then be prompted for the key passphrase as above and the key will be loaded. To check what keys are loaded, right click on the Pageant icon in your tool bar and select "View Keys" or double click the icon to load the interface below.

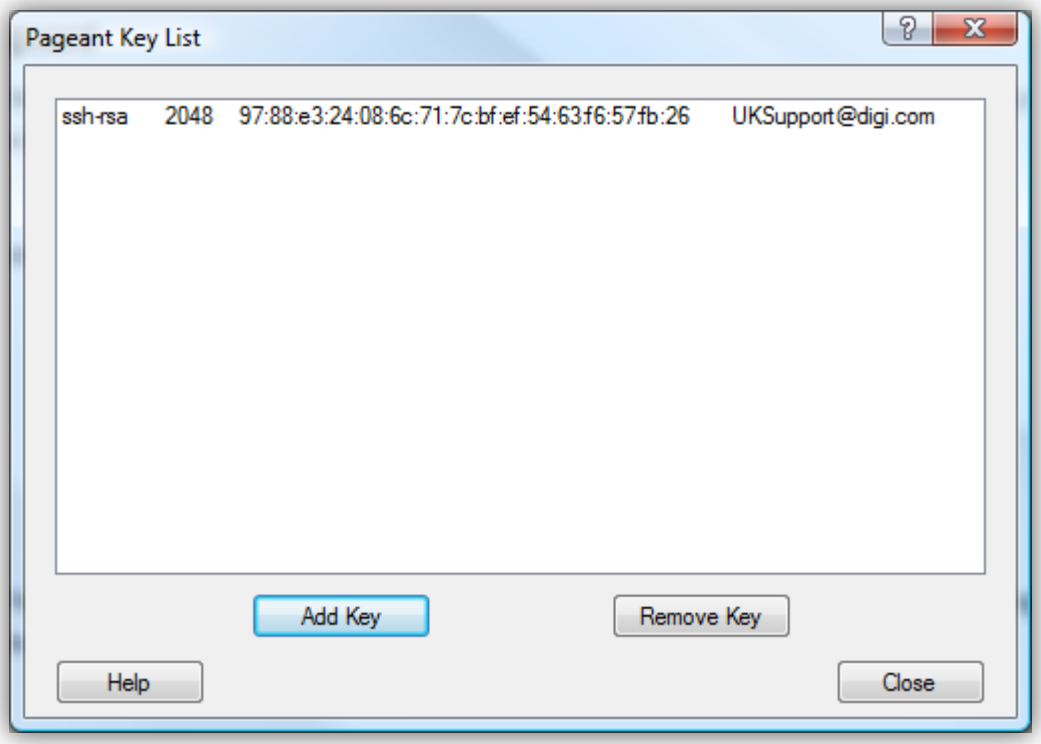

Figure 16: Pageant with SSH private key loaded

As you can see, you can load and remove keys from here in addition to being able to do this via right clicking the Pageant toolbar icon.

5 TEST SSH ACCESS

Open PuTTY and double click on the saved session we setup earlier, that should be shown in the "Saved Sessions" list.

If you are not using Pageant, you will be prompted for a password; if prompted, enter the passphrase that was configured for the private key previously at the PuTTYgen key generation stage above.

Access to the CLI will now be granted.

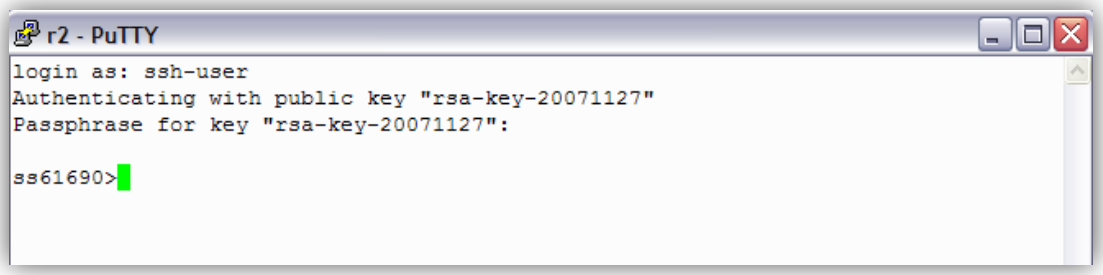

Figure 17: Log into route with SSH key authentication

6 SAVE CONFIGURATION CHANGES TO PROFILE 0

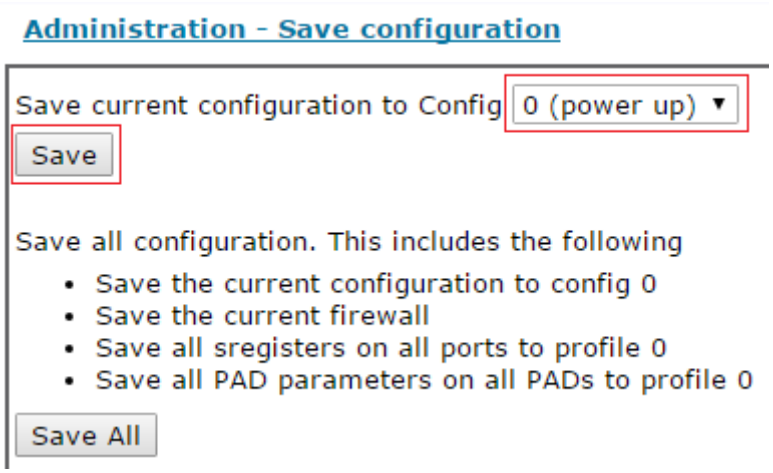

Figure 18: Save config