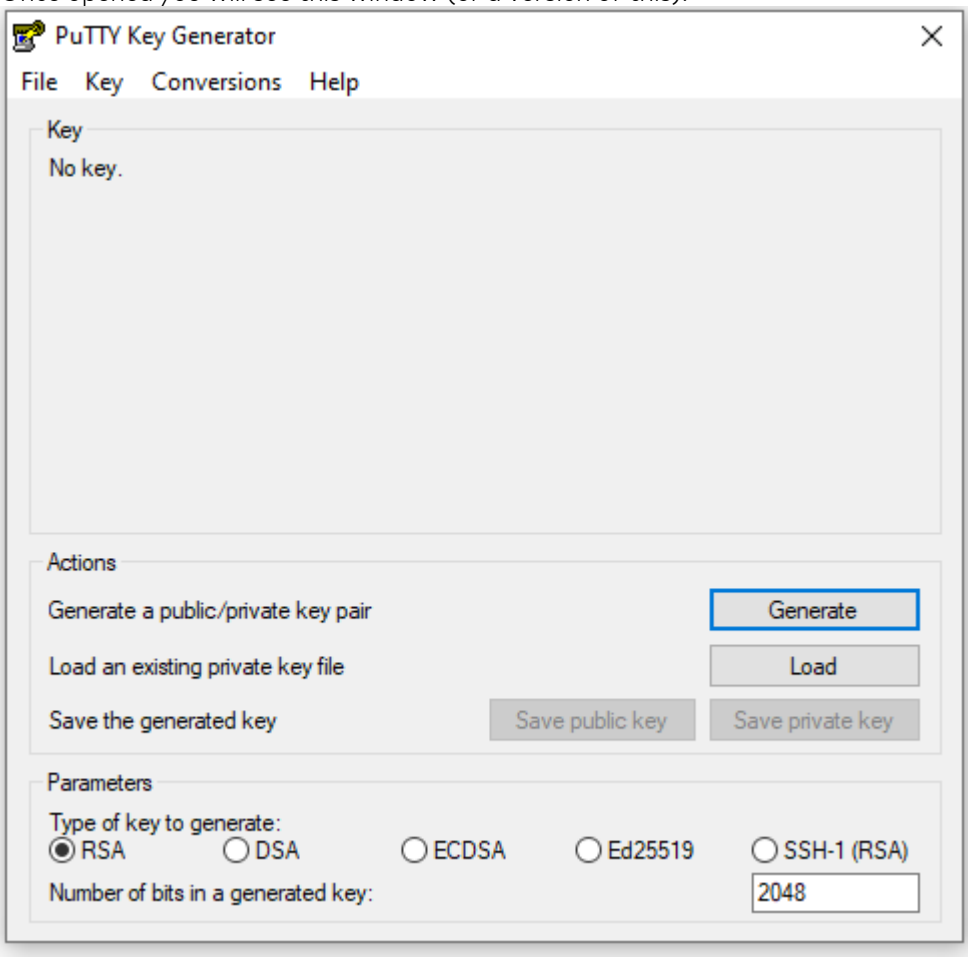
How to generate User Identity Key Pair using PuTTYgen

This guide will show how to use the program PuTTYgen for Windows to create a **User Identification Key Pair** that you can use to authenticate against Mastercard sFTP-server.

Step 1: Open PuTTYgen

Once opened you will see this window (or a version of this).

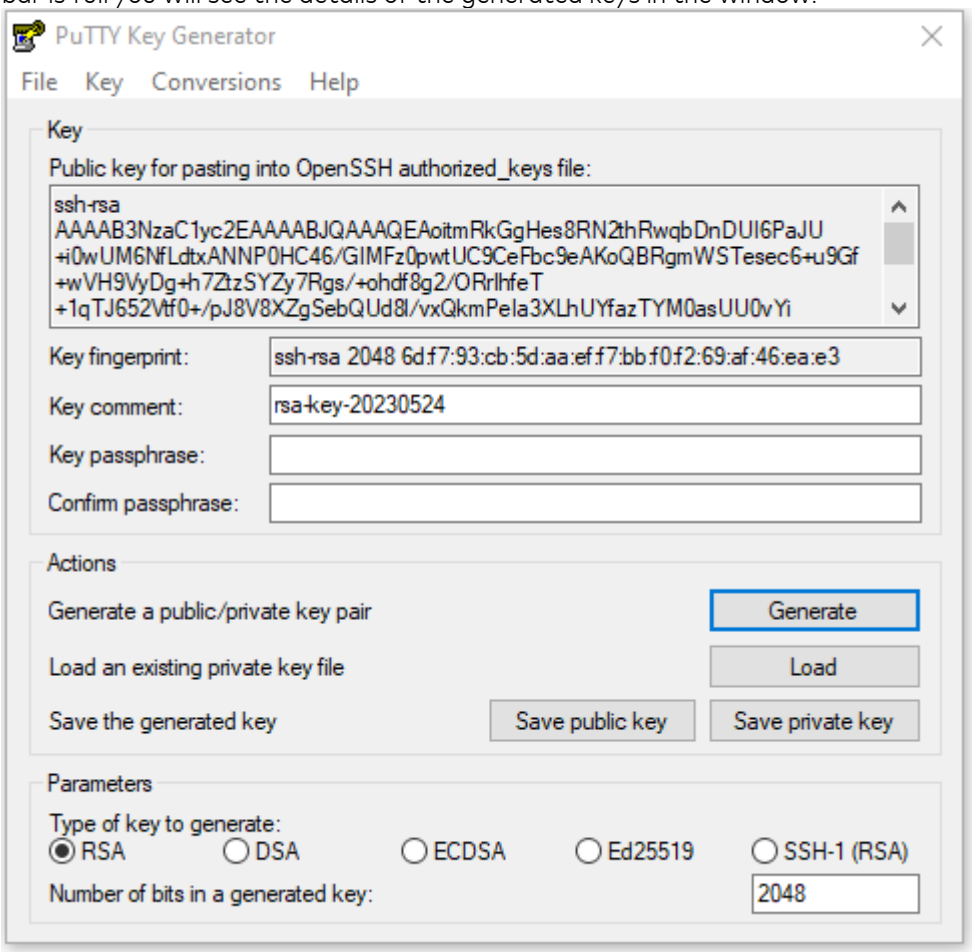


Step 2: Set Parameters for the User Identification Key Pair

At the bottom of the window choose **RSA** as *Type of key to generate* and set *Number of bits in generated key* to **2048**.

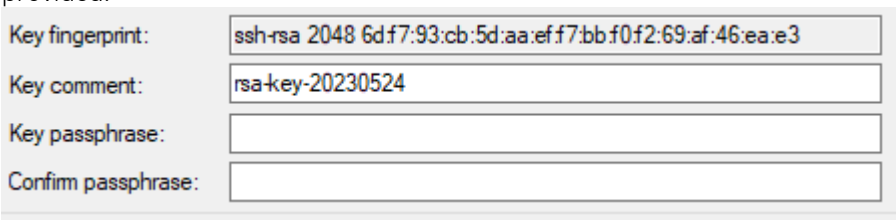
Step 3: Generate the key pair

In the window, under **Actions**, click the button *Generate*. A progress-bar will appear under **Key**. This bar will fill up as you move the mouse-cursor around the empty area in the window below the progress-bar. Once the progress-bar is full you will see the details of the generated keys in the window.



Step 3: Create a passphrase for your key (Optional)

At this point you can create a *Key passphrase* for your private key (the part of the key pair that is used on your sFTP-client). Once a passphrase has been added to the private key, it can only be used if the passphrase is provided.

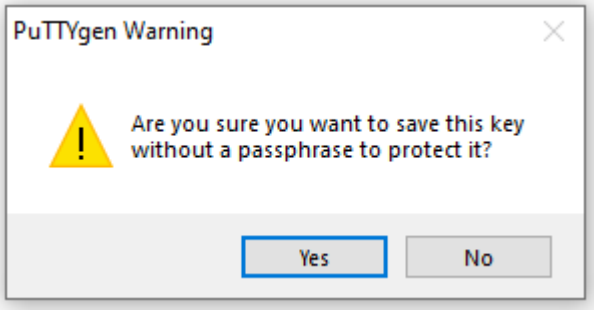


This step is optional, but Mastercard recommends that you add a passphrase to your private key to protect it from unauthorized use.

Step 4: Save your Private Key

Under Actions, click the *Save private key* button.

*If you have NOT added a passphrase to the private key (see Step 3) you will see a prompt asking if you want to save the key without a passphrase. Click **yes** to proceed or **no** to go back to Step 3.



Choose a name for your key and save it.

Step 5: Save your Public Key

Under Actions, click the *Save public key* button. Choose a name and save the key.
** When choosing a name for the keys it can be a good idea to choose a descriptive name and to name the private key and the public key the same way. This makes it easier to see that the two files are connected and what the purpose of the files are.
I.e. you could name the keys Mastercard_sftp_public-key.pub and Mastercard_sftp_private-key.ppk

Step 6: Installing the keys

At this point you should have a working **User Identification Key Pair**. The private key will need to be installed in your sFTP-client program and connect it to the Mastercard connection there. The public key must be sent to Mastercard to be installed on the Mastercard sFTP-server. Once the keys have been installed you should be able to use them to authenticate against the Mastercard sFTP-server and be able create a secure connection.