**DO NOT CALL REGISTER**

**USING SSH KEY FOR SFTP AUTHENTICATION**

The purpose of this document is to provide instructions for Access-seekers on:

* how to generate SSH keys required for SFTP Authentication
* how to provide the SSH keys to the Do Not Call Register for the purpose of connecting to an SFTP Account.

**SSH Keys Generation**

**Generate RSA Keys for Linux**

1. **Generate RSA key** on Linux with **ssh-keygen** as per example below.

It is recommended to enter a passphrase for the RSA key

[tsinoc@debit-inout ~]$ ssh-keygen -t rsa -b 2048

Generating public/private rsa key pair.

Enter file in which to save the key (/home/tsinoc/.ssh/id\_rsa):

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/tsinoc/.ssh/id\_rsa.

Your public key has been saved in /home/tsinoc/.ssh/id\_rsa.pub.

The key fingerprint is:

34:d9:ee:50:83:99:c5:21:70:23:01:d8:7e:c8:6b:b1 tsinoc@debit-inout

1. **Two files will be generated** in the example above:

PRIVATE KEY = id\_rsa located in /home/tsinoc/.ssh/id\_rsa

PUBLIC KEY = id\_rsa.pub located in /home/tsinoc/.ssh/id\_rsa.pub

1. **Save** the **PRIVATE** and **PUBLIC** keys.

Make sure you save the files in the location you remember for later use

[tsinoc@debit-inout ~]$ cat ~tsinoc/.ssh/id\_rsa.pub

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAgEA7sykiS0yBPbPKfrG6F9qw8EuWXAgF1NvajvkZuXM0nhD73dcMKIKKOFNMBf4meiEhW5hj/wpZD7LzPTqhPny88RCwG2LTGaUYyAOFJgaS5G/4GA6j5gdcmWMAbITMFWOnzlUsHRPp57Oc2CSWLmteahDBY6PS5tBkwevS/0bnh75ae7EmO3Uy6JOBCrHoHS8J5VyjPX3y45USWiDlcKPMu3X42S5Wa8jcjEjbK9/DQtR+K2XilH4K6bHd7UsgRCFFnCviCimKVxhbdynv1R4PE5wybf56ZQG3n9GpSACvm6X5Jtb63lrnnDBqBNP+wEMUJkyU7lIRwvSFRQEXJij9C2iVQIIMwBlLQGGM+oGIDbYgH7C5SxRafWZf/91RUL5JwzdUVnz2+R4as/PYzClPdB40XNL/TJTr7XJBD+O/oBoPStXEBozHOEbfVs6w2AZ7lcSQGD0bSSDXXmJsAncw51OP8TBucb0AVtZrrOeRwv6zmtM/BJwJYNE/KEXWtN4Tn/9mQzzciikJJW5I4rNsSbgymJ8GnBlgxTWXbWdauxafyUPMWmvw4ii7u5VRA/ibrYS2172cVKj4XTxR9sCQpO08w52pKBAKxqoJSh804iI33aAHcQSWVDe4aH7a/Rmc6fuzW6aubxB4YsLi7gxmjuqer2UkSWRus9IehdCDOk= tsinoc@debit-inout

**Generate RSA Keys on Windows using PuTTY Key Generator**

1. **Download** the executable **PuttyGen** file from:
<http://the.earth.li/~sgtatham/putty/latest/x86/puttygen.exe>
2. Go to **Windows > Search Programs and files >** **puttygen.exe.**



1. Make sure the **Type of key to generate is SSH-2 RSA** and the **number of bits** **in a generated key** is **2048** (as per above).

**Click** > **Generate**.

Make sure to constantly move the mouse around, otherwise key generation will stall

1. Click on **'Save public key'** then **select** and **Copy the Public key** (as per below).

It is recommended to enter a passphrase for the keys generated



1. **Open Notepad** and **paste** the copied **public key**.
2. Click **Format** > Make sure that **Word Wrap** under the Format menu **is UNCHECKED.**
3. **Save** the **public key**.

Save the file to the location you will remember for later use



1. Last time from PuttyGen is to save your private Key.

Click on **'Save private key'.**

Save the file to the location you will remember for later use

 

**Public Key Delivery**

The saved **PUBLIC KEY** should be provided to the Do not Call Register by **uploading** it to the **Upload folder** of the SFTP server after connecting to the designated account.

Both Public and Private keys will be later used to connect to the SFTP Server

**Uploading Public Key on Linux**

1. **Connect** to the **SFTP -** **sftp.donotcall.gov.au -** server using your **username** and **password**.
2. **Change** tothe **Upload** directory**.**
3. **Upload Public Key.**

salmat@ubuntu:~/.ssh$ sftp 00000@sftp.donotcall.gov.au

00000@sftp.donotcall.gov.au's password:

Connected to sftp.donotcall.gov.au.

sftp> dir

archive download upload

sftp> cd upload

sftp> put id\_rsa.pub

Uploading id\_rsa.pub to /upload/id\_rsa.pub

id\_rsa.pub 100% 399 0.4KB/s 00:01

sftp>

**Uploading Public Key on Windows using WinSCP**

1. **Connect to the SFTP** - **sftp.donotcall.gov.au** server using your **username** and **password**.



1. Click **Yes** on the **Warning** below. 

1. Go to the **Upload** directory.



1. **Upload Public Key** into **Upload** folder.

