

a.- Generating the public and private key

- Using PuTTYGen (Windows)
 - Generate Key Pair using the PuTTYGen application
 - Save the Key Pair
- Delivery of the public key to WIPO

Using PuTTYGen (Windows)

PuTTYGen can be installed separately or together with WinSCP (Free Windows SFTP/SCP client)



It can be downloaded from :

As part of WinSCP - downloaded from <https://winscp.net/>

or

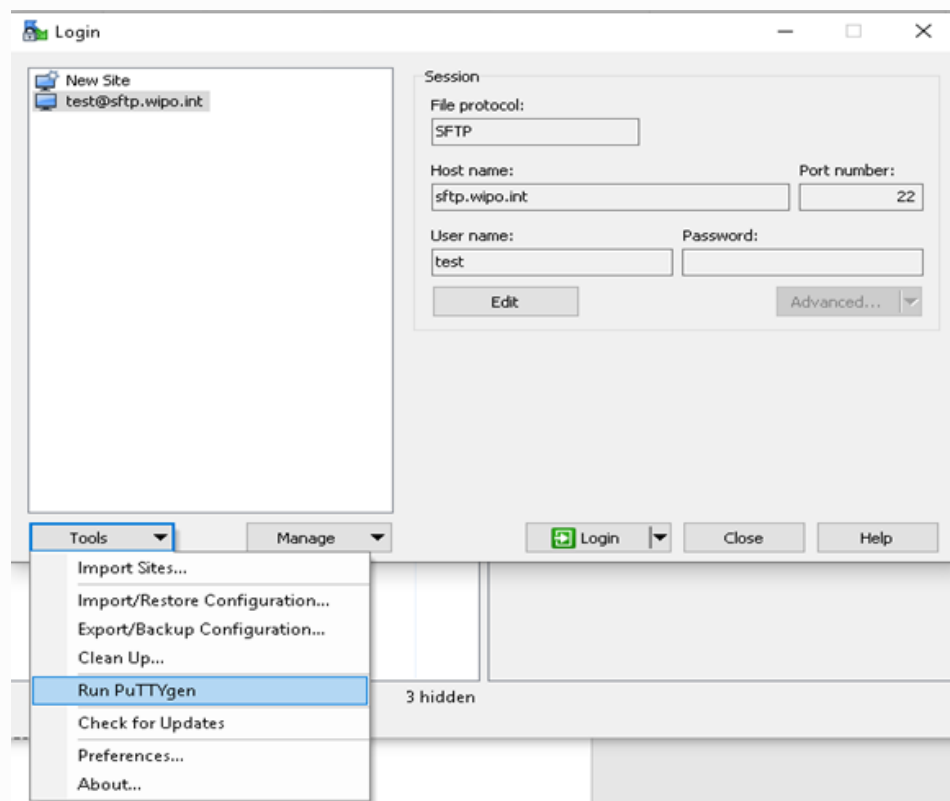
PuTTYGen(alone) - download from <https://www.puttygen.com/>

After downloading the package, run it.

If you chose WinSCP, select your desired language and then select "Typical Installation", which includes PuTTYgen and Pageant. Follow the installation instructions.



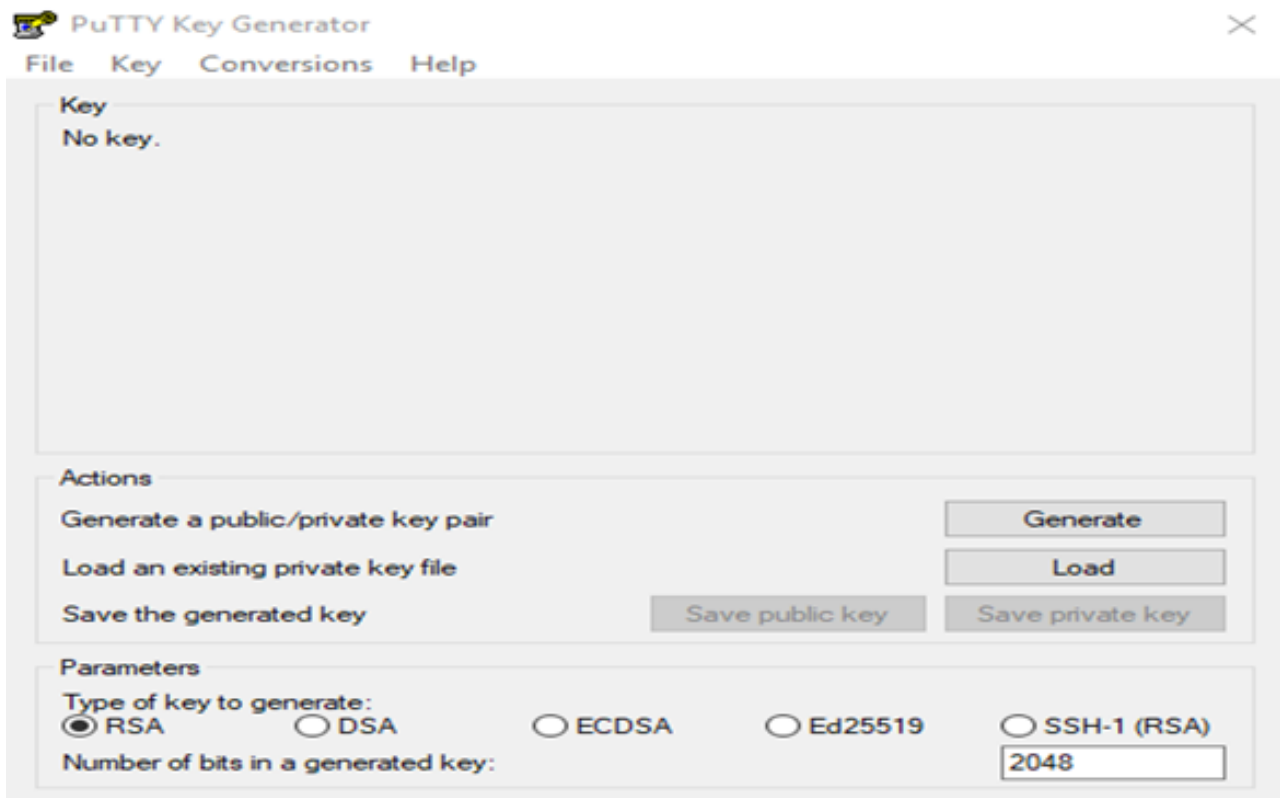
For WinSCP, after installation finishes, you can find PuTTYGen in the menu:



Generate Key Pair using the PuTTYGen application

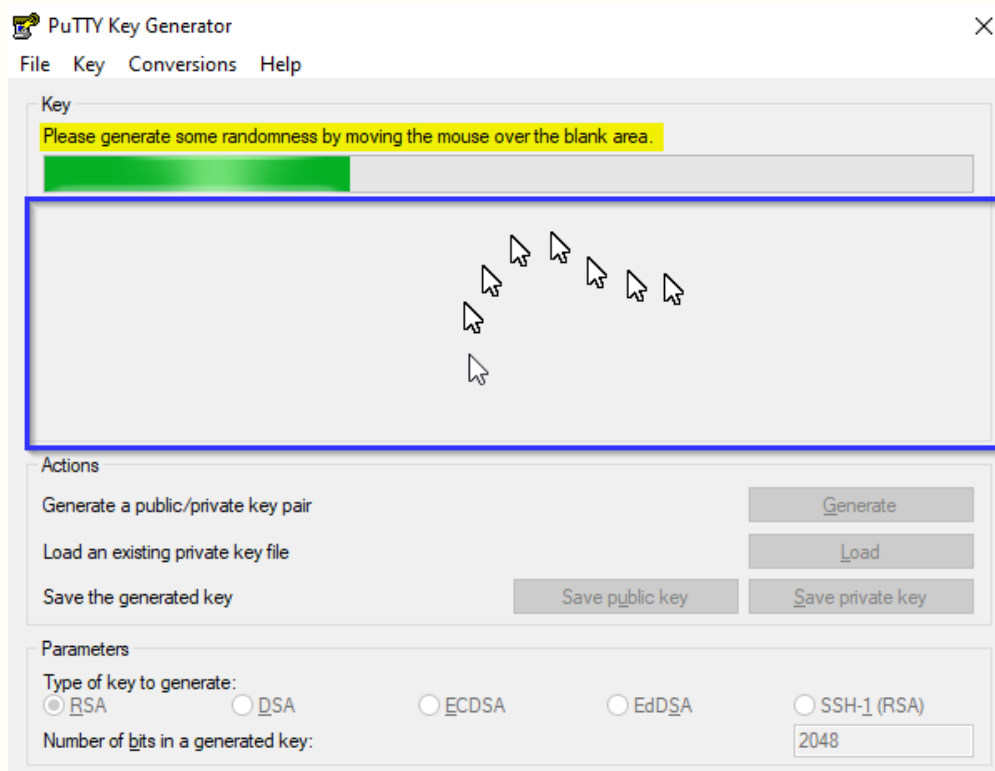
In both cases the PuTTYGen usage is the same, it is used to create the authentication keys as explained below:

- Select "RSA" for the "Type of key to generate", with 2048 bit key size or greater.
- Press the "Generate" button and follow the instructions on the screen.



Important

Please note that, as indicated, you will need to move the mouse cursor within the indicated area in order to complete the process:



- When the key generation is complete, the screen looks like below:

PutTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAAQEAhEpwssmps4nfw82LB/jBDL94PmlAW/zG/BgJi
rZeVG+XXh71afgr5Y2jBns2EqUxsh5WTe2xYn
+eoh2iX0K5lpNeBAw12e9t0/wMbiV2tJfxyCXsZX1psA0wL2rRBOoOkhyppRJDPPr/RO
TJmLeM
```

Key fingerprint: ssh-rsa 2048 de:a6:d4:f8:4c:70:fc:fa:12:63:dd:4d:05:87:dc:6b

Key comment: rsa-key-20190819

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate: ☒ RSA ☐ DSA ☐ ECDSA ☐ Ed25519 ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

- Enter a strong passphrase and **remember it**. You will be prompted to type it when you use this key. The passphrase is never sent to the remote server.

Save the Key Pair

1. Press the **"Save public key"** button to save your public key. Name it using the suggested account name, with the extension ".pub" (Example: *ipob_jsmith.pub* or *ipob_cr.pub*)
2. Press the **"Save private key"** button to save your private key. Give it the same name but with ".ppk" extension (*ipob_jsmith.ppk* or *ipob_cr.ppk*)

PutTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDb92UpIOhT9n0LGJFaU7DI/RWhoN4SkwYBo08UdCNatpBvsJpvQ
/g5SagAOd8CVh9MVL5ZdMN1ymq8TPFKxLMscF1v93MZVnM/JoiBW2eLCU8mvYcXm/fGSP8aRktocyBGnU
sTPpHHdue5nGQQOeoH6s5YPhF8ZAxCRcV0UF9tEgZqmSInf4LR1QhxAL1HXP1ALh26o7vy3S+hwuDbI/Foh
+/ga03/BQ1wjAQo1Hstqy77Q4lb1/GEFF8rK4zx+B8tTP87rm0u6ntK2d9AGVDIG
```

Key fingerprint: ssh-rsa 2048 SHA256:NvjklLv/zwm/zBLFBONS3/vjPN1LzG9uDxLfT7hBTM

Key comment: rsa-key-20240201

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate: ☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048



Be aware that the format of the key should only be RSA SSH2.

If you view the public key with a text editor, will look like something like this:

```
1  ---- BEGIN SSH2 PUBLIC KEY ----
2  Comment: "rsa-key-20200929"
3  AAAAB3NzaC1yc2EAAAABJQAAAQEAiVqHjz/BttZOetV0G/Wctfyy1m+f5RMTz1bS
4  +bSG1zWgf5He9zmq46y/B2pVxY7UxQWD5C/xdV5s/P+h+KuOD7NM4ARZFF7VozeH
5  8UW2G06U5+sdkfjasldkfjslospdfsdi21323sfZL2MNBiiIWg2YR15GQI1K73kO
6  2at7Kv0B193qr97ZXpE2/mmxQlgZ2GVLZBJM+e0qGqS0irDzPjwDGLr9qExsli39
7  1foDoSDYvIr8y6e+ktE1vxAQr48xiY13Ybils92gpcbkPO1xMw+2Tdid8qTAV1zm
8  uuWdogFceh+nDn9lZTE8Vm2sUu2R+/E00HexT/EH+0aARCRhhw==
9  ---- END SSH2 PUBLIC KEY ----
```

Be aware that the sequence of characters will be different and unique (is random characters generated by the process described above).

Delivery of the **public key** to WIPO

Rename the files using the suggested account naming convention.



Account Naming Convention

Example for individual:

- Private Key: **ipob_jsmith.ppk**
- Public Key: **ipob_jsmith.pub**

Example for IPO (using country or organization two-letter code according to [WIPO ST.3](#)):

- Private Key: **ipob_cr.ppk**
- Public Key: **ipob_cr.pub**



Email your **public key** to your support contact copying the ipas mailbox (ipas@wipo.int).



NEVER SEND THE PRIVATE KEY! Keep it safe.