

Creating & Using SSH Keys on Windows

1. Download and Install Putty

<https://www.chiark.greenend.org.uk/~sgtatham/putty/>

PuTTY: a free SSH and Telnet client

[Home](#) | [FAQ](#) | [Feedback](#) | [Licence](#) | [Updates](#) | [Mirrors](#) | [Keys](#) | [Links](#) | [Team](#)
Download: [Stable](#) · [Snapshot](#) | [Docs](#) | [Changes](#) | [Wishlist](#)

PuTTY is a free implementation of SSH and Telnet for Windows and Unix platforms, along with an xterm terminal emulator. It is written and maintained primarily by [Simon Tatham](#).

The latest version is 0.71. [Download it here.](#) 

LEGAL WARNING: Use of PuTTY, PSCP, PSFTP and Plink is illegal in countries where encryption is outlawed. We believe it is legal to use PuTTY, PSCP, PSFTP and Plink in England and Wales and in many other countries, but we are not lawyers, and so if in doubt you should seek legal advice before downloading it. You may find useful information at cryptolaw.org, which collects information on cryptography laws in many countries, but we can't vouch for its correctness.

Use of the Telnet-only binary (PuTTYtel) is unrestricted by any cryptography laws.

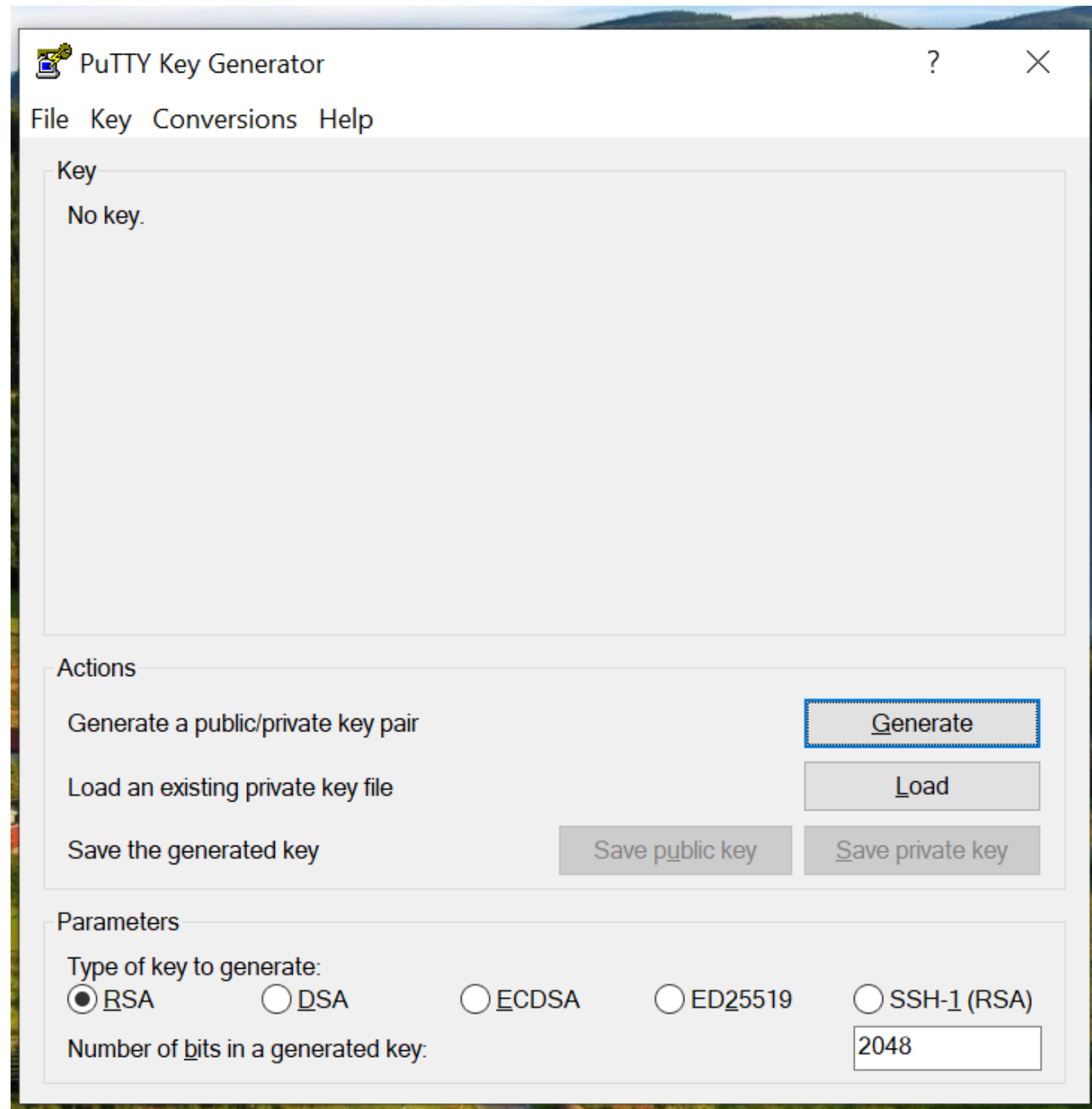
Latest news

2019-03-25 Bug bounty continues

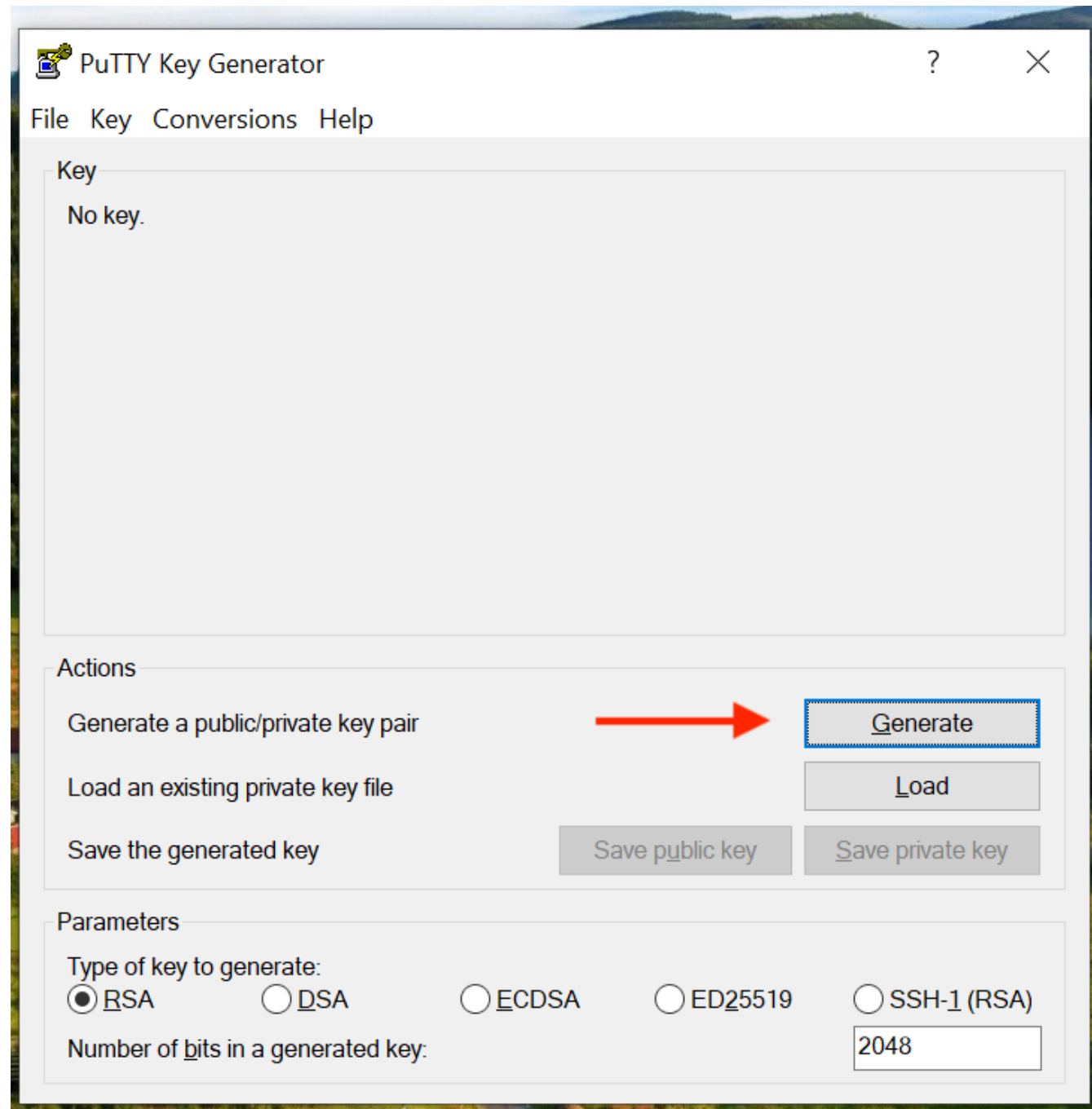
This year's EU-funded bug bounty programme is **still running**. It was originally scheduled to end on 7th March, but there was money left over in the budget. So while that money lasts, you still have a chance to earn some by finding vulnerabilities in PuTTY 0.71 or the development snapshots!

As before, vulnerabilities should be reported through the [HackerOne web site](#) in order to qualify for a bounty: if you send reports directly to the PuTTY team in the usual way then we'll still fix them but we can't provide

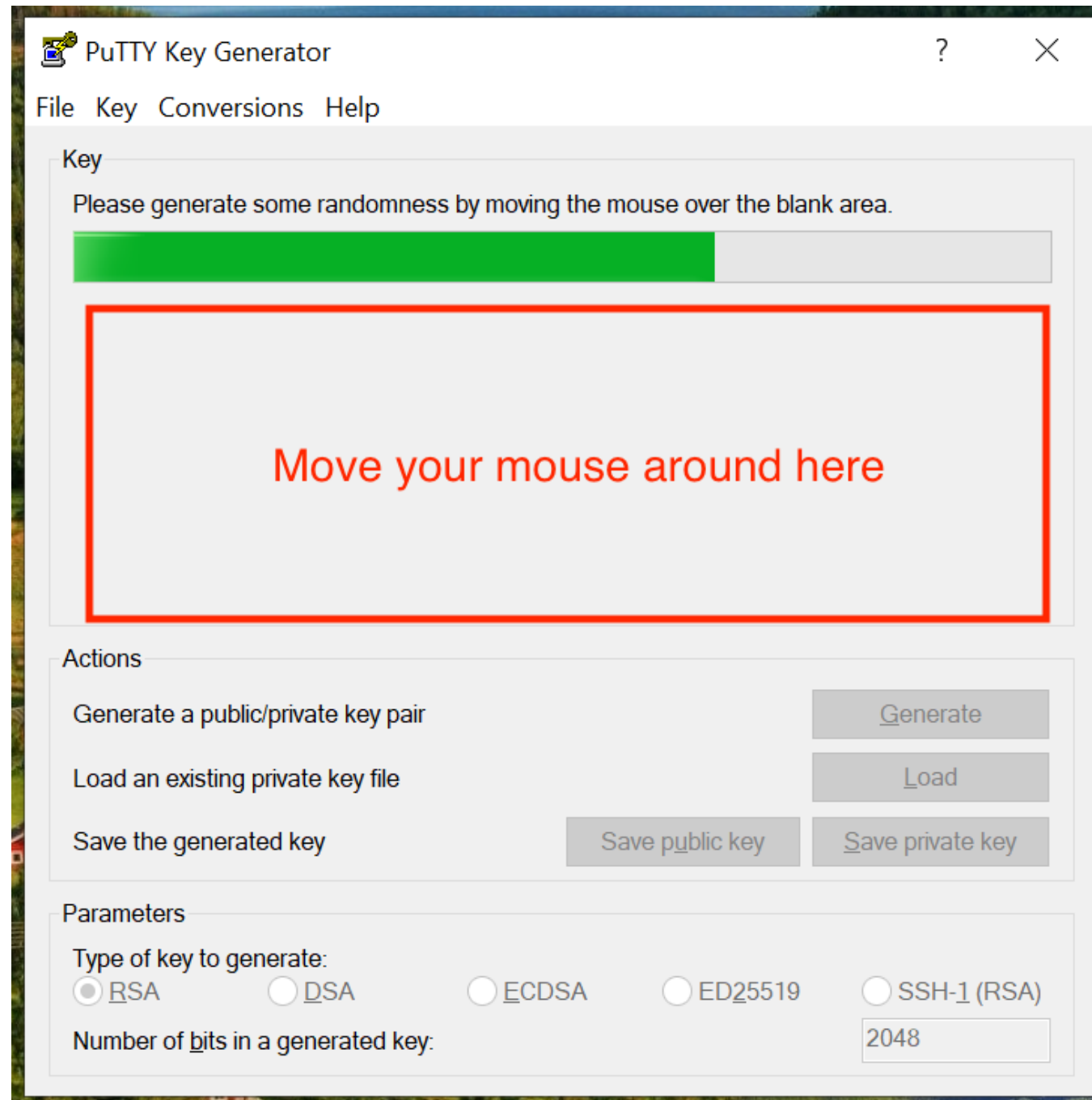
2. Launch *PuTTYGen*



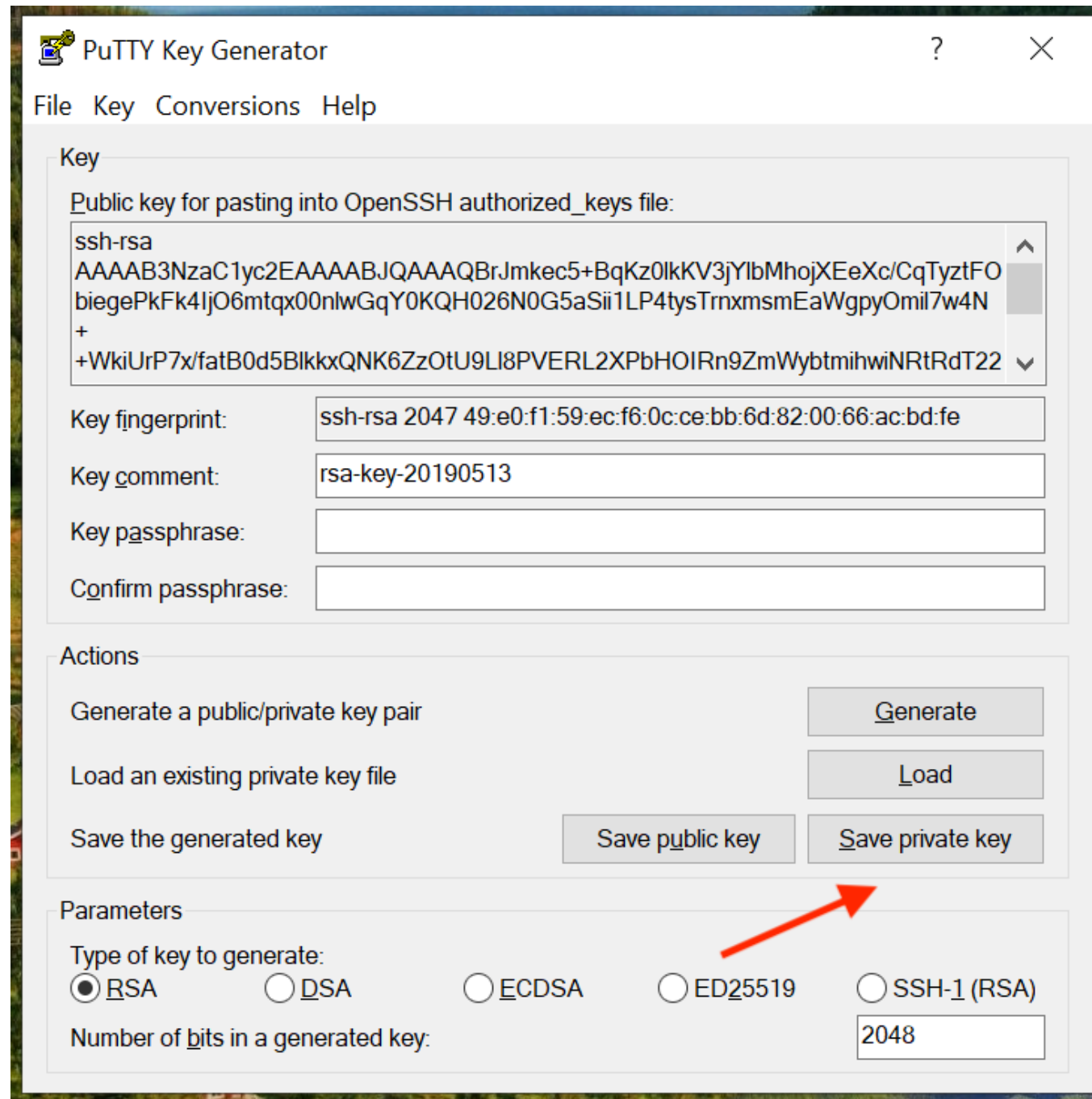
3. Click *Generate*



4. Wiggle your Mouse



5. Save Your Private Key



PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQBrJmkec5+BqKz0lkKV3jYlbMhojXEeXc/CqTyztFO
biegePkFk4ljO6mtqx00nlwGqY0KQH026N0G5aSii1LP4tysTrnxmsmEaWgpyOmi7w4N
+
WkiUrP7x/fatB0d5BlkkxQNK6ZzOtU9LI8PVERL2XPbHOIRn9ZmWybtmihwiNRtRdT22
```

Key fingerprint: ssh-rsa 2047 49:e0:f1:59:ec:f6:0c:ce:bb:6d:82:00:66:ac:bd:fe

Key comment: rsa-key-20190513

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:

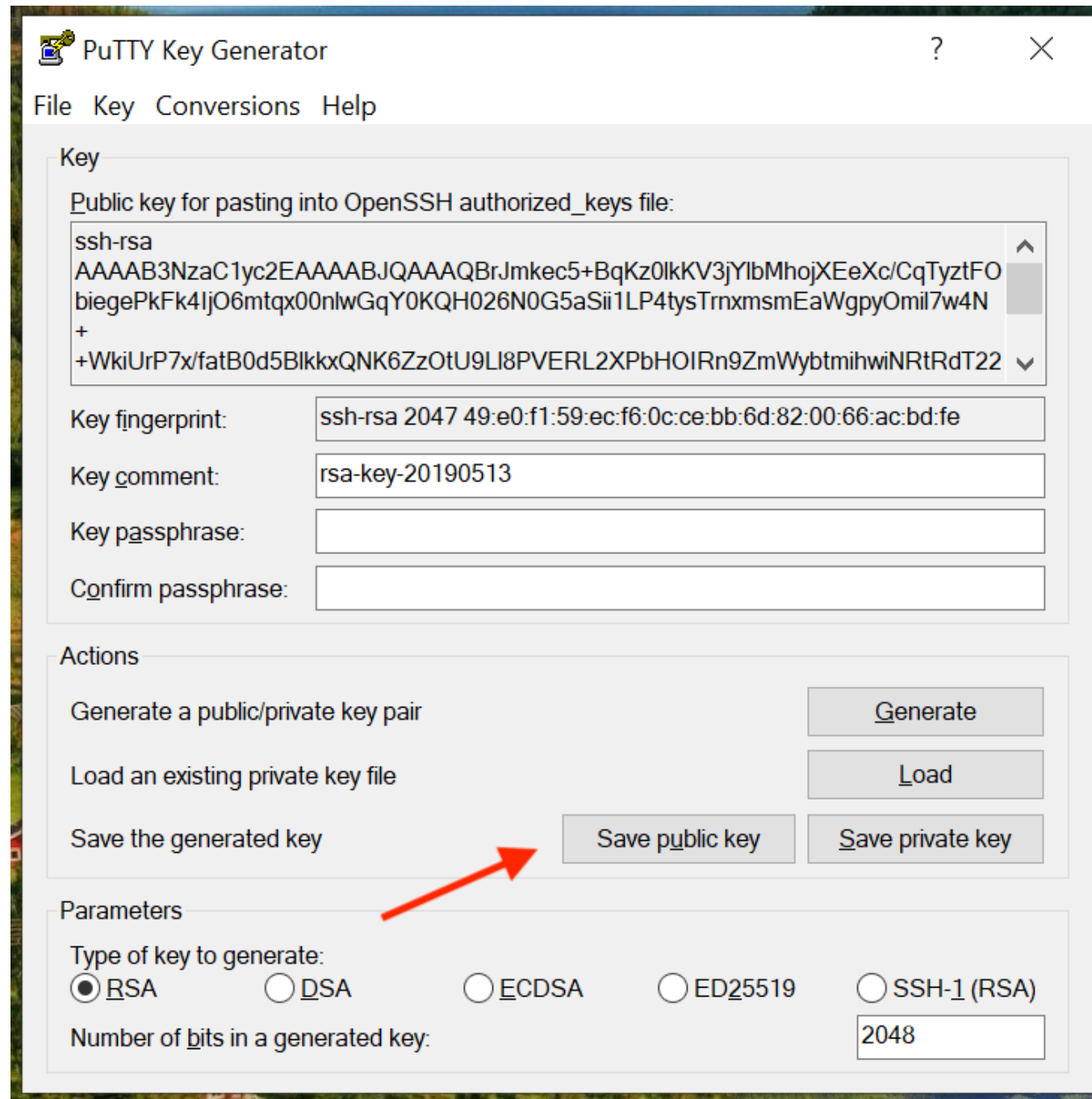
☒ RSA ☐ DSA ☐ ECDSA ☐ ED25519 ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

Save it anywhere
you'd like and
remember the
directory

we'll be using it later

7. Save Your Public Key



The screenshot shows the PuTTY Key Generator window. The 'Key' section displays the public key for pasting into an OpenSSH authorized_keys file. The 'Actions' section contains buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'. A red arrow points to the 'Save public key' button. The 'Parameters' section shows the key type set to RSA and the number of bits set to 2048.

PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQBrJmkec5+BqKz0lkKV3jYlbMhojXEeXc/CqTyztFO
biegePkFk4ljO6mtqx00nlwGqY0KQH026N0G5aSii1LP4tysTrnxmsmEaWgpyOmi17w4N
+
+WkiUrP7x/fatB0d5BlkkxQNK6ZzOtU9LI8PVERL2XPbHOIRn9ZmWybtmihwiNRtRdT22
```

Key fingerprint: ssh-rsa 2047 49:e0:f1:59:ec:f6:0c:ce:bb:6d:82:00:66:ac:bd:fe

Key comment: rsa-key-20190513

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

Save it anywhere
you'd like and
remember the
directory

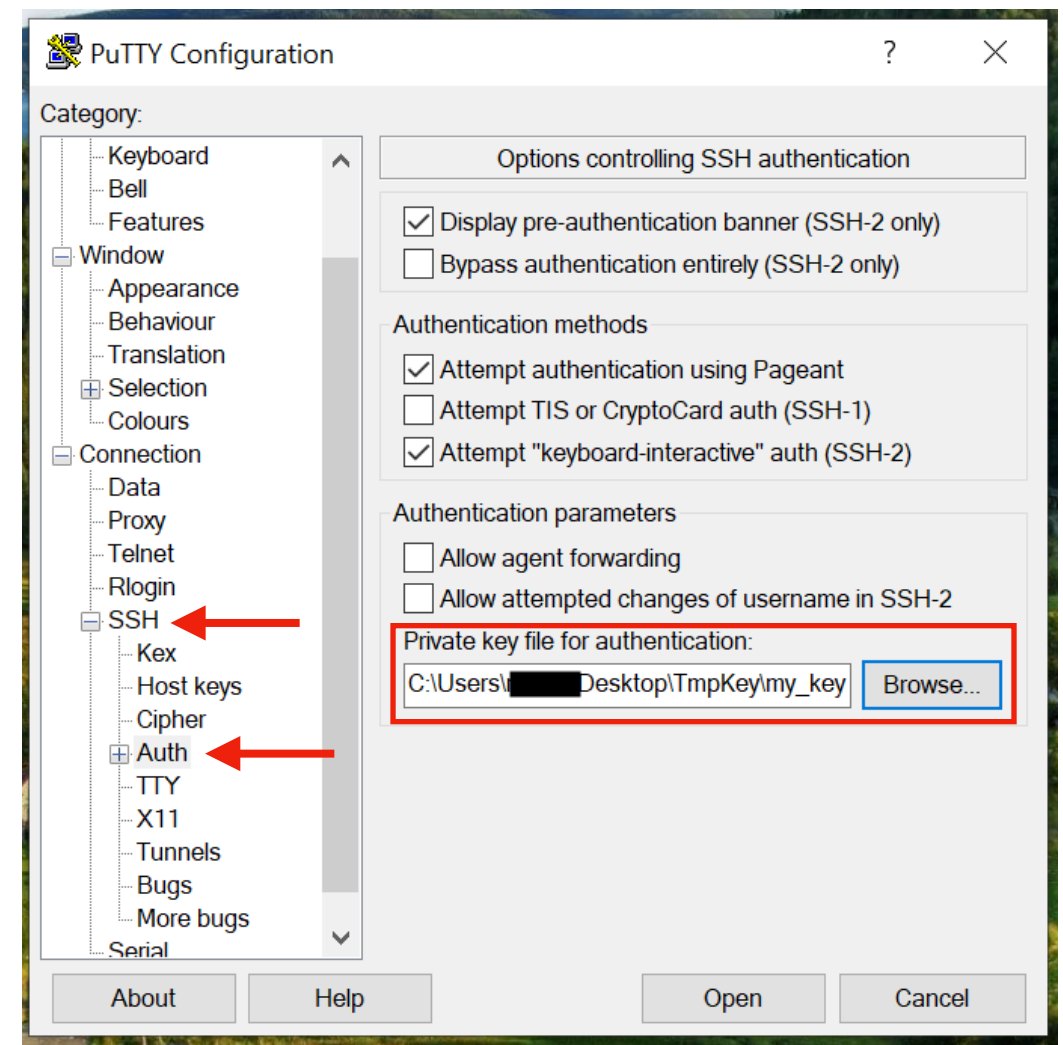
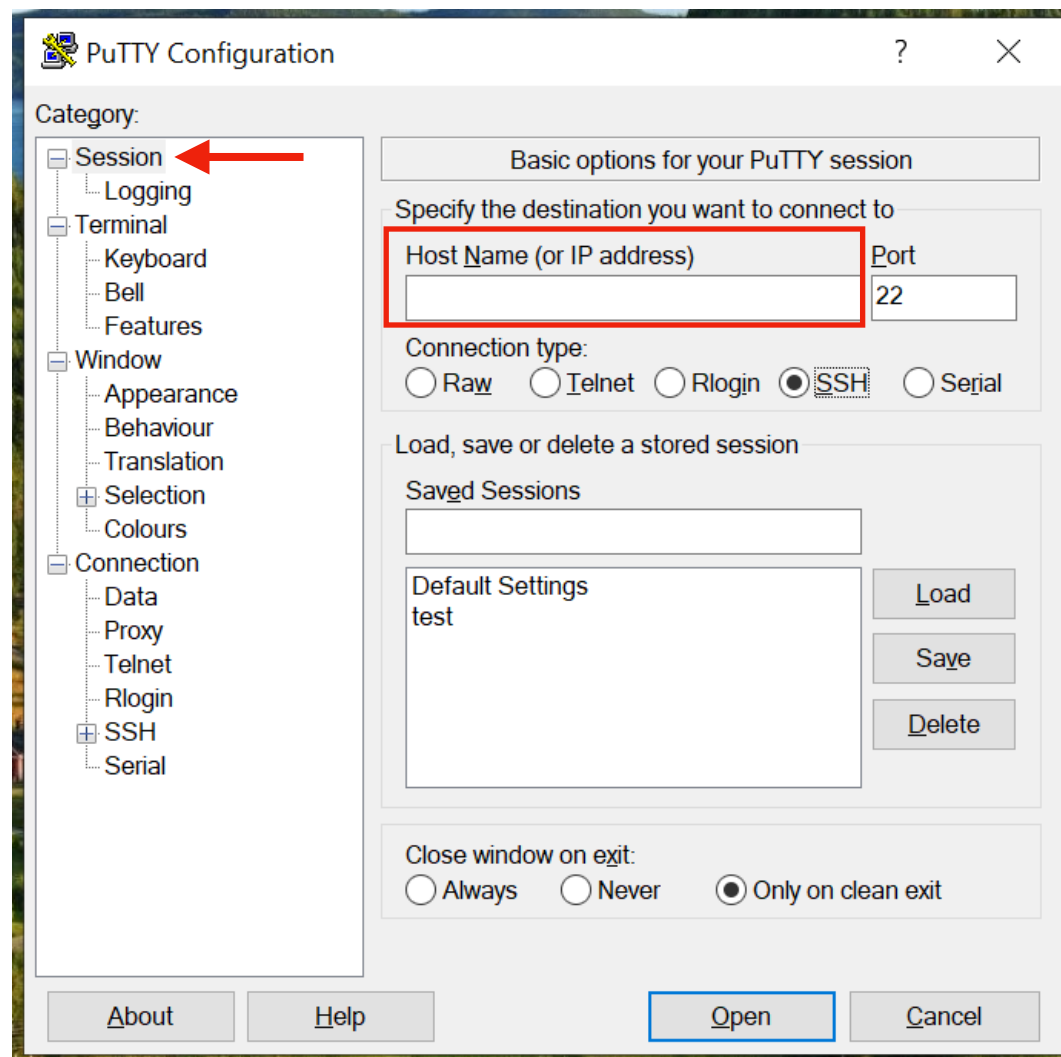
we'll be using it later

8. Use Your Key Pair in Putty

Open Putty (not PuttyGen)

Enter IP address of remote machine

Add the *private* key by browsing to the key you just saved and open a new connection



Notes

- You'll need to import your *public key* into AWS in order to access EC2 resources (add it in "Keys" under EC2 portal)
- In Step 5, we did NOT save a passphrase with the key; using a passphrase is more secure, but requires you enter the phrase every time you log in
- Your *public key* can be given out freely; that's why you can safely upload it to AWS
- Keep your *private key* safe on your local system