

# LHB Private and public SSH Key Configuration

## Purpose

The purpose of this document is to help N3C sites or the data managers create/set up private and public SSH keys. The keys are required to access the Linkage Honest Broker (LHB) SFTP for submission of the transit tokens/metadata files. This document provides instructions how to configure the keys for SFTP on Windows or MAC operating system.

## Initial Setup

The Linkage Honest Broker hosted by Regenstrief Institute uses a data inbox upon which your organization will upload files via Secure File Transfer Protocol (SFTP). After creating a zip file which contains the Transit Tokens generated using the Datavant tool, you will submit that content to your data inbox at the LHB site. During this load the following steps occur:

1. The new zip file is checked for conformance ( TO DO: add the link to file format specs)
2. The encrypted tokens are extracted and stored so that they can be linked with other sites.
3. Any new zip file uploaded with the same name of the last one will be reprocessed.

These Files will remain in your inbox. We are working on a retention policy as once the file is processed for tokens, the original zip file is no longer needed by our system.

The inbox / SFTP does not require the use of passwords. Instead, it uses a **public/private key** protocol for secure data transfer.

## Overview of this process

1. Install required software applications
2. Create a Public / Private Key pair for secure connection
3. Submit your Public key only to the LHB
4. Setup Filezilla SFTP client secure connection to our data inbox

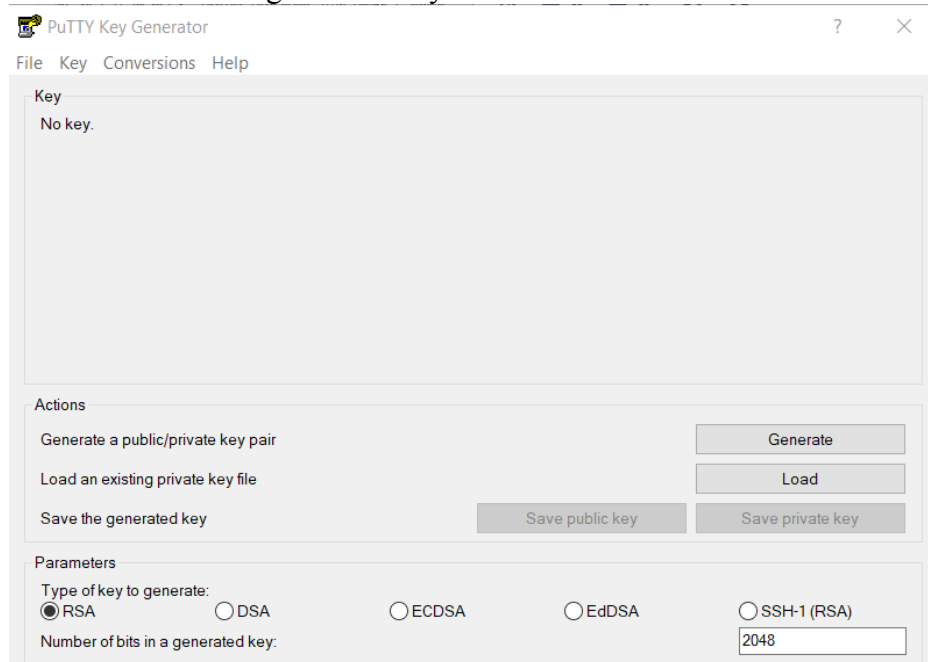
## Prerequisites

Install the required tools:

1. PuTTY (for Windows OS)  
- <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>
2. FileZilla (for Windows and Mac OS) - <https://filezilla-project.org/download.php?type=client>

## Creating a Public / Private key: Windows Instructions

1. Install PuTTY
  1. 64 bit is sufficient
2. Once installed, go to Windows Start Menu → All Programs → PuTTY → PuTTYgen
3. Under Actions, click **Generate** button to create the Public and Private Keys
  1. Type of Key to Generate - RSA
  2. Number of bits in a generated key - 2048



4. Move the mouse within the window. Putty uses mouse movements to collect randomness. The exact way you move your mouse cannot be predicted by an external attacker. You may need to move the mouse for some time, depending on the size of your

key. As you move it, the green progress bar should advance.

The screenshot shows the PuTTY Key Generator application window. The title bar reads "PuTTY Key Generator" with a question mark and a close button. The menu bar includes "File", "Key", "Conversions", and "Help". The main window is divided into three sections: "Key", "Actions", and "Parameters".

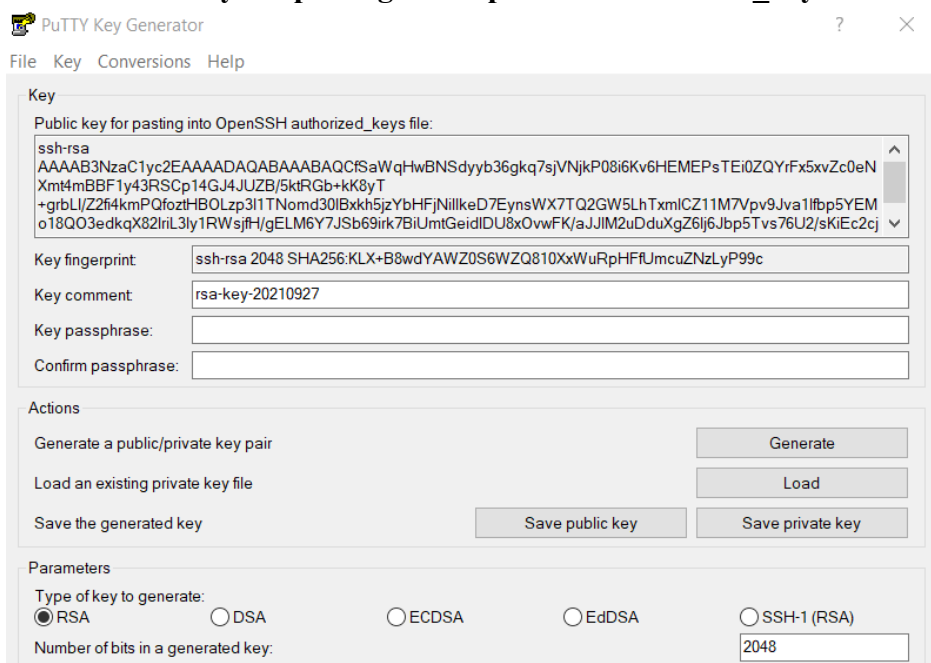
The "Key" section contains the instruction "Please generate some randomness by moving the mouse over the blank area." Below this is a horizontal progress bar that is partially filled with green. The rest of the section is a large, empty gray area.

The "Actions" section contains four buttons: "Generate", "Load", "Save public key", and "Save private key". The "Generate" button is positioned to the right of the text "Generate a public/private key pair". The "Load" button is to the right of "Load an existing private key file". The "Save public key" and "Save private key" buttons are positioned to the right of "Save the generated key".

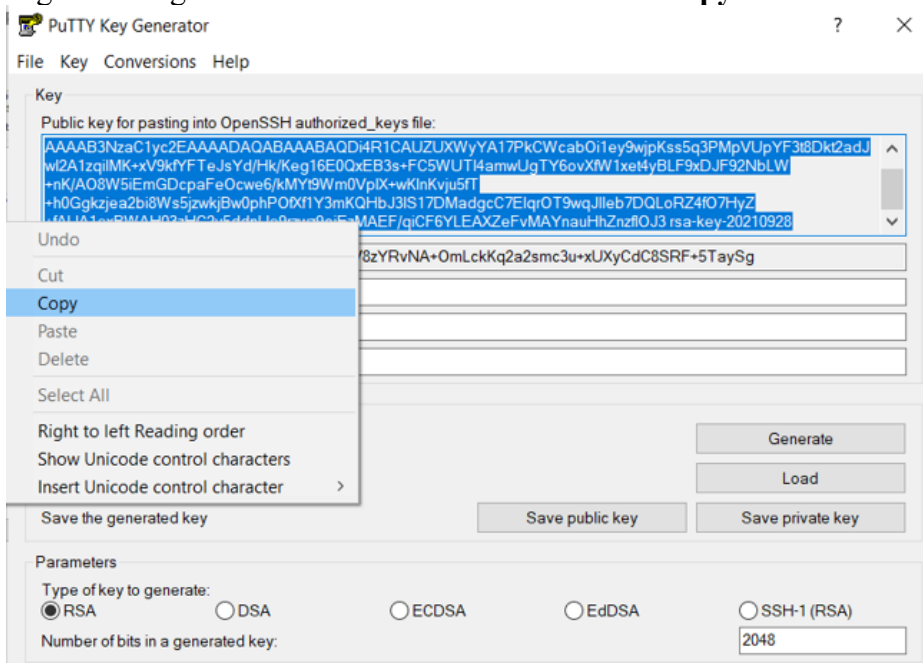
The "Parameters" section contains two rows of options. The first row is "Type of key to generate:" with five radio buttons: "RSA" (selected), "DSA", "ECDSA", "EdDSA", and "SSH-1 (RSA)". The second row is "Number of bits in a generated key:" with a text input field containing the value "2048".

5. Once the progress bar becomes full, the actual key generation computation takes place. This may take from several seconds to several minutes. The Public Key will be displayed

in the **Public Key** for pasting into OpenSSH `authorized_keys` file



6. *Optional*: Enter a specific passphrase for the key. We strongly recommended using a passphrase for private key files intended for interactive use. If keys are needed for automation, they may be left without a passphrase.
7. Right click where it says **Public Key** for pasting into Open SSH `authorized_keys` file and choose **Select All**.
8. Right click again in the same text field and choose **Copy**




9. Open **Notepad** or other text editor and paste the public key by right clicking and selecting **Paste**.
10. Go to **File** → **Save As**.

1. **File Name:** LHB\_LastName\_publickey (example: LHB\_smith\_publickey)
2. **Save as type:** .txt
3. Click **Save** (*Tip:* Save to Desktop as this is needed to upload to the Individual User Access Form (REDCap))

File name:	lhb_smith_publickey.txt
Save as type:	Text Documents (*.txt)

11. Go Back to PuTTYgen to save your **Private Key** by clicking the **Save Private Key** button

 PuTTY Key Generator ? ×

File Key Conversions Help

**Key**

Public key for pasting into OpenSSH authorized\_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAkELmTLwXzvetvCyVN2rziG4+cFBUT/bKfJecYckXtCnKY
+NnYitUTc7RIICUJF2nNS4za5W
+b7rL9/Tc8iXRMT1h4CWq3JUUp0a9OnHOlzGuqUr2B6l0itlBhsRb9iFQCHEUaDt73L9pn1CkzUmZxsAT0+eKquUglXWZ4fF
X+KEwFPzQz9jnM9rPDR8D9ctKcbAg9EvD3rJvThii2F96Ue2gyiNvegZpFYsxyG0qaOEohz+U
+/T08T21puy0GijxeCwZpgwaaaSplKIPcHiMRufOCref/jkUNMkv6JUXtNZ2yYc3PoDIF4MEj30G3bqqqT6IXZXZbFJfIXRfM3
```

Key fingerprint: ssh-rsa 2048 SHA256:wmMUUBnLYAaDzJabnJwf8laKDFK6xwMUiSjKSn5r6ml

Key comment: rsa-key-20210929

Key passphrase:

Confirm passphrase:

**Actions**

Generate a public/private key pair Generate

Load an existing private key file Load

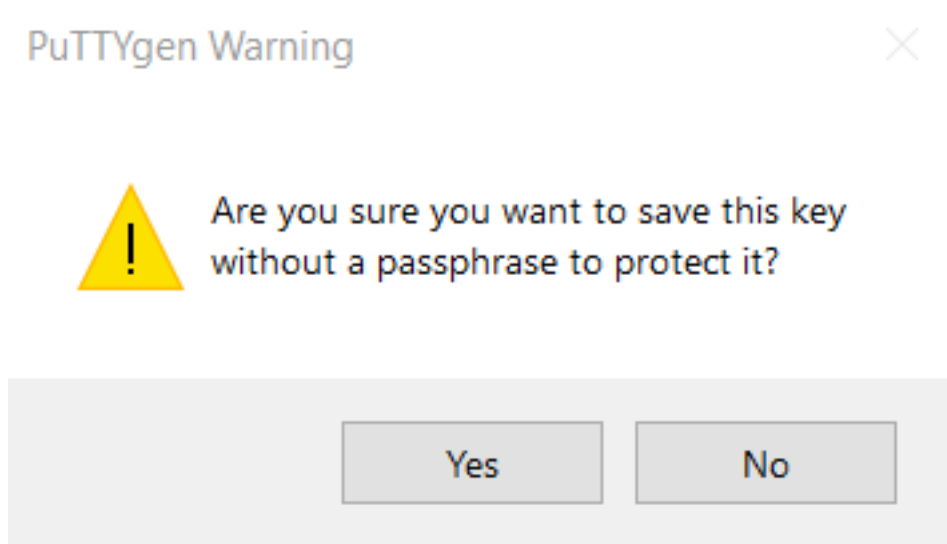
Save the generated key Save public key **Save private key**

**Parameters**

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

Number of bits in a generated key: 2048

12. A **PuTTY Warning** dialog box will display - user does not need to create a passphrase.  
Click **Yes** to continue



13. Create a file name for your Private Key and make sure **".ppk"** is the extension (ex: PrivateKey.ppk) and click

**Save**

A screenshot of a "Save" dialog box. It has two fields: "File name:" with the text "private key" and a dropdown arrow, and "Save as type:" with the text "PuTTY Private Key Files (\*.ppk)" and a dropdown arrow.

14. After saving the file, the **Save Private Key** dialog box will close.  
1. **NOTE:** Do *not* share, e-mail or send private key to anybody.

## Send your Public Key to Regenstrief (LHB)

Attach the Public SSH Key file named *lhb\_<last name>\_publickey.txt* to the Individual User Access Form provided via e-mail from the Linkage Honest Broker ([rillhb@regenstrief.org](mailto:rillhb@regenstrief.org)). There is a specific field in the form for you to attach the file.

---

## Creating a Public / Private key: Mac Instructions

Mac OS has built in tools to generate the private/public keys. Below are instructions to create the private and public SSH keys

### 1. Open a terminal

Terminal is the terminal emulator which provides a text-based command line interface to the Unix shell of macOS. To open the macOS Terminal follow these steps:

1. In Finder, choose **Utilities** from the **Applications** folder
2. Find **Terminal** in the Utilities list.

### 3. Open **Terminal**

The Terminal window opens with the command line prompt displaying the name of your machine and username.

## 2. Generating an SSH Key

An SSH key consists of a pair of files. One is the private key (do not share with anybody) and the other is the public key. The public key allows you to log into the LHB SFTP. When you generate the keys, you will use ssh-keygen to store the keys in a safe location so you can bypass the login prompt when connecting to the SFTP.

**To generate SSH keys in macOS, follow these steps:**

1. Enter the following command in the **Terminal** window
  1. ssh-keygen -t rsa
    1. This starts the key generation process. When you execute this command, the ssh-keygen utility prompts you to indicate where to store the key.
2. Press the **Enter** key to accept the default location. The ssh-keygen utility prompts you for a passphrase
3. Type in a passphrase. You can also hit the Enter key to accept the default (no passphrase). However, this is not recommended.
  1. You will need to enter the passphrase a second time to continue
4. After you confirm the passphrase, the system generates the key pair.
5. Your private key is saved to the id\_rsa file in the .ssh directory and is used to verify the public key.
  1. ***Never*** share your private key
6. Your public key is saved to the id\_rsa.pub file and is required to be uploaded to the Individual User Access Form (REDCap form)

**To find your SSH keys in macOS, follow these steps:**

1. Go to Finder → Go.
2. Select **Go to Folder**
3. In Keygen copy and paste the **Created Directory** into the text box. Ex:  
/users/firstnamelastname/.ssh
  1. Your user library opens so you can review contents
4. Click **Go**
5. The .ssh folder will open
  1. Your private and public keys will be in this folder.
  2. Rename the Public Key (file ends in .pub) with LHB\_LastName\_PublicKey.pub
6. The key fingerprint is:  
SHA256:Y0FkVU0AnfrHv9CpJlZ+nBN+6Gu/dRGPie7QM3I6fq4 <username>

## 3. Provide Public Key to Linkage Honest Broker (LHB)

Attach the Public SSH Key file named *lhb\_<last name>\_publickey.pub* to the Individual User Access Form provided via e-mail from the Linkage Honest Broker (rilhb@[regenstrief.org](mailto:rilhb@regenstrief.org)). There is a specific field in the form for you to attach the file.

---