Lab: Generating SSH Keys on Windows

Overview

SSH (or *Sec*ure *SH*ell) keys provide us with a high-security protocol that allows us to authenticate without using a password. Some roles require SSH keys in order to access different servers/services. In order to connect to those services you'll need to create and enroll your own set of keys.

Each set of keys consists of two long strings of characters, a public key and a private key, which will be protected with a passphrase (or password). You place the public key on remote servers you need to access while the private key remains on your local system. When the public and private key matches, the system is unlocked.

To learn more about public-private key cryptography, you can watch the SysComm Deep Dive: OpenSSL video (1:01).

Objectives

Upon successful completion of this lab, you will have successfully

1. generated public and private SSH key pairs,
2. uploaded your public keys and had them verified by the NOCC, and
3. add your keys to your session.

Prerequisites

Security Awareness Policy

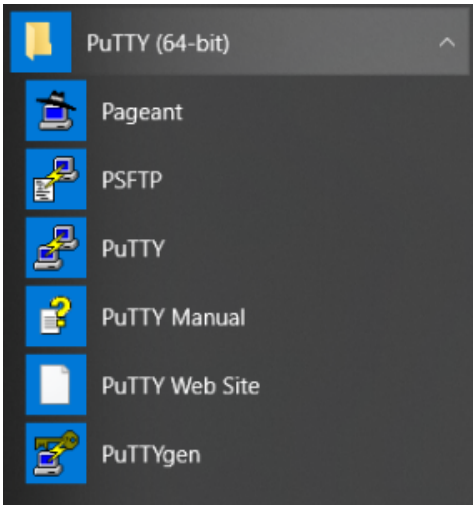
Before we can begin you'll need to review and accept the Akamai Security Awareness Policy (if you have not done already). This document covers important information about protecting Akamai data, and acceptance is required in order to obtain SSH keys.

Key Management Policy

Because SSH keys can give individuals access to potentially sensitive information and systems you'll need to review and accept the Key Management Policy (if you have not done already) before continuing.

Required Software

Login to the Akamai IT Solution Center with your Akamai username and password (for "Organization" select "Default") then go to the software downloads page. Click on the latest release of PuTTY which should download a Windows installation image file (putty-64bit-x.xx-installer.msi where x.xx is the version) to your designated downloads file on your Windows machine. After the download is complete, use the Windows File Explorer to navigate to that file then double-click on it to start the installation process. After successful installation, you will see the PuTTY tools in your start menu.



Important Considerations

Keys generated by the PuTTY utility on Windows are in a format incompatible with the OpenSSH format used on MacOS and Linux / UNIX systems. However, PuTTY is able to save keys in that format, which you will do.

Kinds of Key Pairs

There are four different types of key pairs that we use at Akamai. Depending on your role, you may need more than one set.

Internal	External	Deployed	Protected
Provides access to machines within the corporate network. This includes Perforce, lab machines, and other hosts that are managed internally. Everyone should generate this kind of key.	Allows access to gateways: • callahan.akamai.com (East US) • caldecot.akamai.com (West US) • chowk.akamai.com (Bangalore)	Used to access LSGs and to gwsh to machines on the deployed network, additionally they can be used in config. other* as allowed by authgate grants.	Protected keys are for NOCC personnel only, and used for the same type of access as a Deployed key. Protected keys can only be used at a NOCC workstation.

Your manager will inform you if you should generate keys other than internal.

Generate Public and Private Key Pairs

1. Using either File Explorer, a DOS window or Windows PowerShell terminal window, create a directory called `ssh_keys` under the C: drive. This is where the keys will be stored.

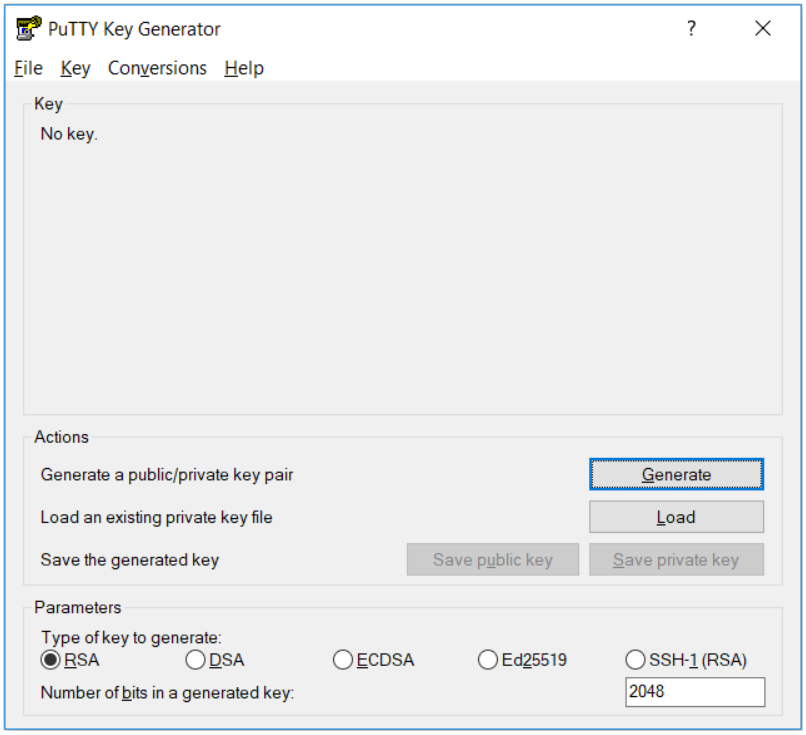
   ```
   > mkdir C:\ssh_keys
   ```

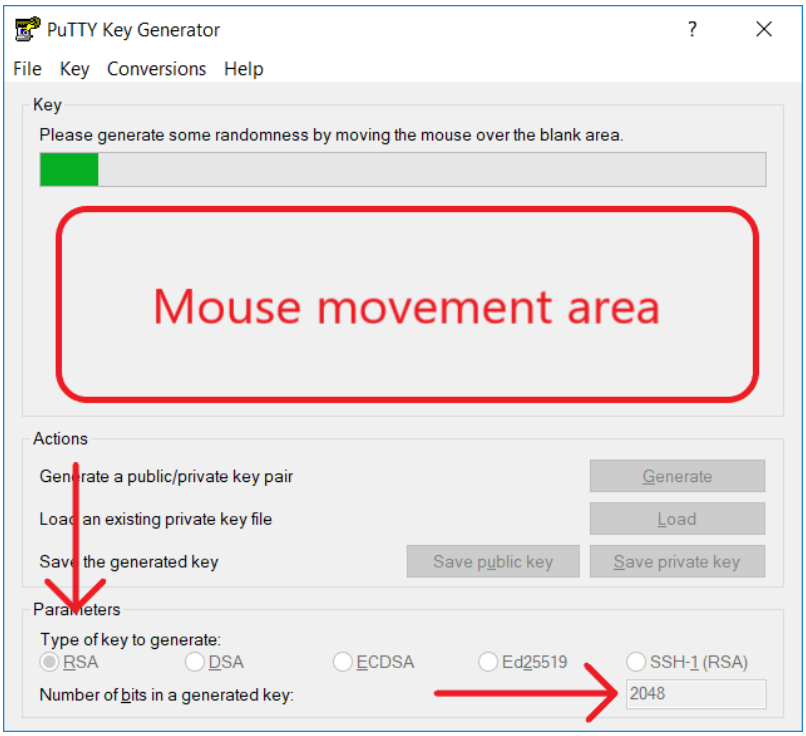
2. Use PuTTYgen to generate the keys.

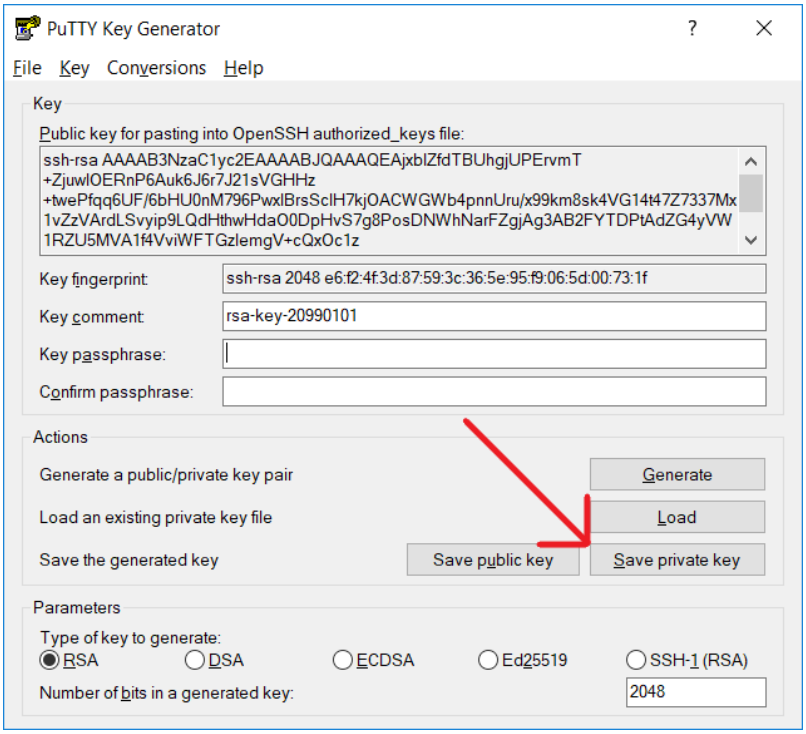
   The placeholder [key-type] represents the type of key and will either be “internal”, “external”, “deployed”, or “protected”.
   Repeat the step below for each type of pair you need to generate, substituting the proper value for placeholder [key-type].

   a. Generate a PuTTY private key.
      i. Ensure that "RSA" is selected for the type of key [*NOT* SSH-1 (RSA)] and the number of bits is set to 2048.

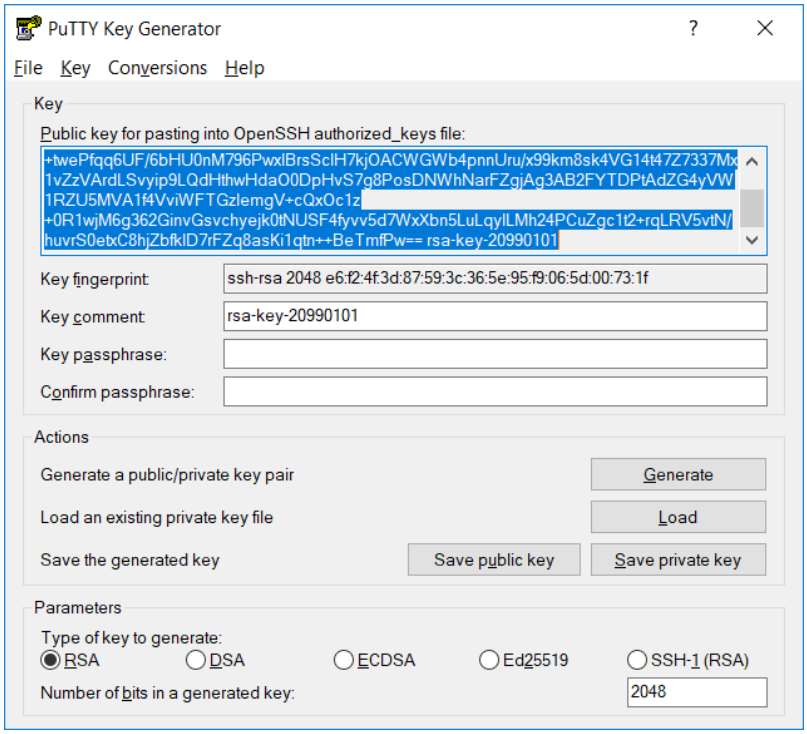
ii. Click the "Generate" button to start the process. PuTTYgen will prompt you to continuously move your mouse over the blank area of the box above the "Generate" button until the key generation is complete, which will introduce randomness used to generate more secure keys.
iii. Verify you see in the "Key fingerprint" box a string that begins with "rsa-ssh 2048" followed by a hexadecimal string. If you see anything else, click "Generate" and repeat the two steps above. This hexadecimal string is the MD5 digest of the key. You will need this string when you confirm your key with the NOCC.
iv. In the "Key comment" box, enter the following: "<username>-[key-type]-windows-yyyymmdd" where "<username>" is your Akamai username "yyyymmdd" is today's date.
Note that today's date (in the format yyyymmdd) is most likely already there.
v. Enter a very strong passphrase (something longer than a typical password). Your passphrase should conform to Akamai's Key Management Policy. The idea is to enter a phrase that will thwart a brute force / dictionary attack for a prohibitively long time. You shall not leave this blank!
vi. Enter the same passphrase in the "Confirm passphrase" box. Please note that passphrases are unrecoverable. If you forget your passphrase, a new key must be generated and uploaded to the NOCC.
vii. Click on the "Save private key button." Navigate to the directory you created previously, C:\ssh_keys, and save this private key with the filename "<username>-[key-type]-windows-yyyymmdd" (same as the "Key comment" from above). The program will automatically add the extension ".ppk" for "PuTTY Private Key."


PuTTY Key Generator
File Key Conversions Help
Key
No key.
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

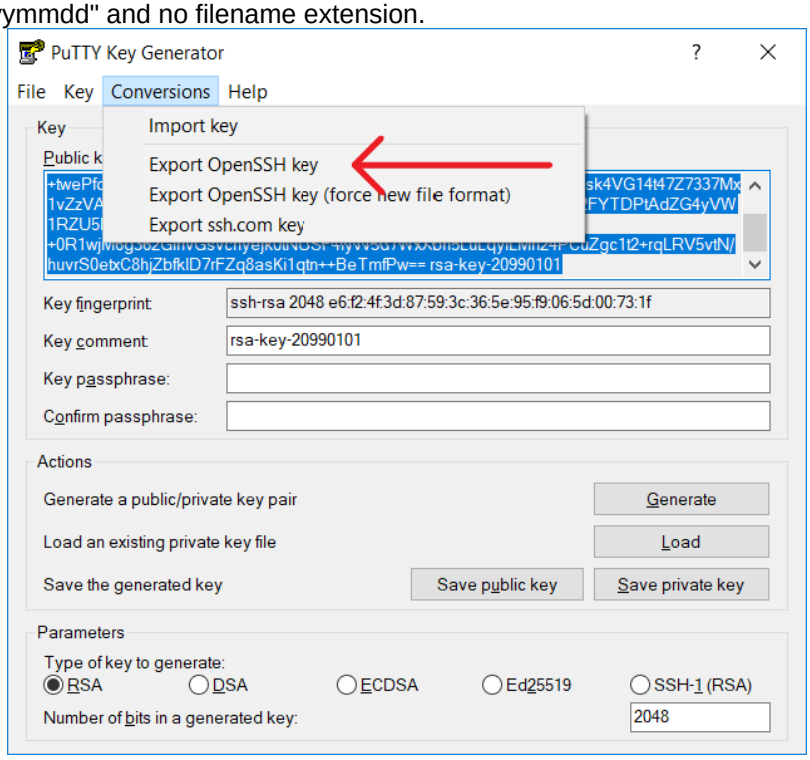

PuTTY Key Generator
File Key Conversions Help
Key
Please generate some randomness by moving the mouse over the blank area.
Mouse movement area
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA Ed25519 SSH-1 (RSA)
Number of bits in a generated key:
2048



b. Generate the public key. This key will be compatible with the OpenSSL format.
    i. Select then copy all the text in the "Public key for passing into OpenSSH authorized_keys file" box.
    ii. Open a text editor, typically Notepad: Press the Windows key and "r". In the resulting dialog box, type "notepad" then press "OK".
    iii. Paste the selected text into Notepad. At the very end of the text, press the "Enter" key to add a newline character to the end of the text.
    iv. Save the file in the same location as the private key (C:\ssh_keys) using the filename "<username>-[key-type]-openssh-yyyymmdd.pub". Note everything is the same, except the "windows" part is changed to "openssh".



c. Generate an OpenSSL-compatible private key from your PuTTY private key.
   i. From the menu in the PuTTYgen window, select Conversions Export OpenSSH key.
   ii. In the resulting file dialog box, save this public key with the filename "<username>-[key-type]-openSSH-yyyymmdd" and no filename extension.



3. List the contents of the key directory to verify you have keys using a DOS window, PowerShell terminal, or File Explorer.

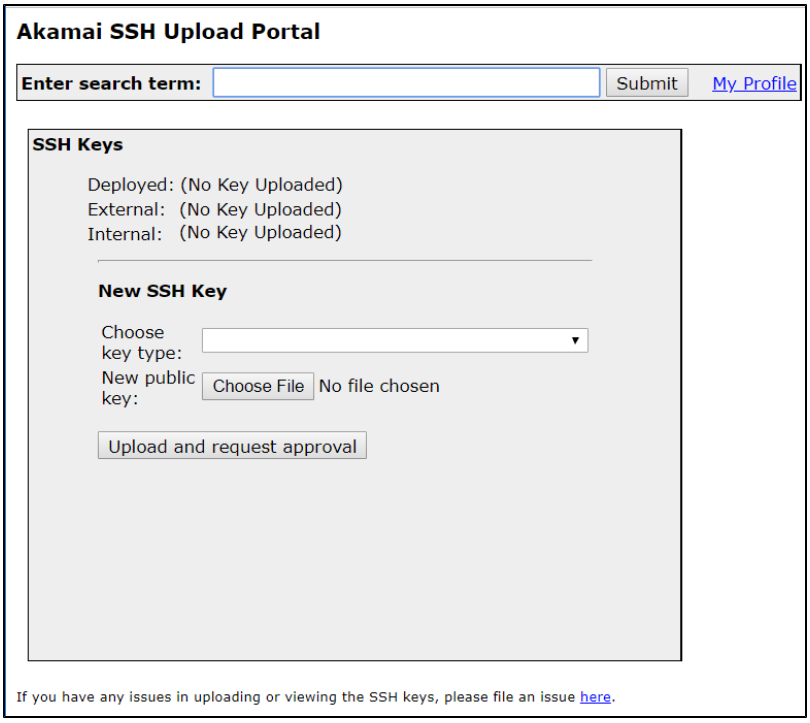
```
> dir C:\ssh-keys
<username>-internal-openSSH-2099-01-01  <username>-internal-windows-2099-01-01.ppk  <username>-internal-windows-2099-01-01.pub
```

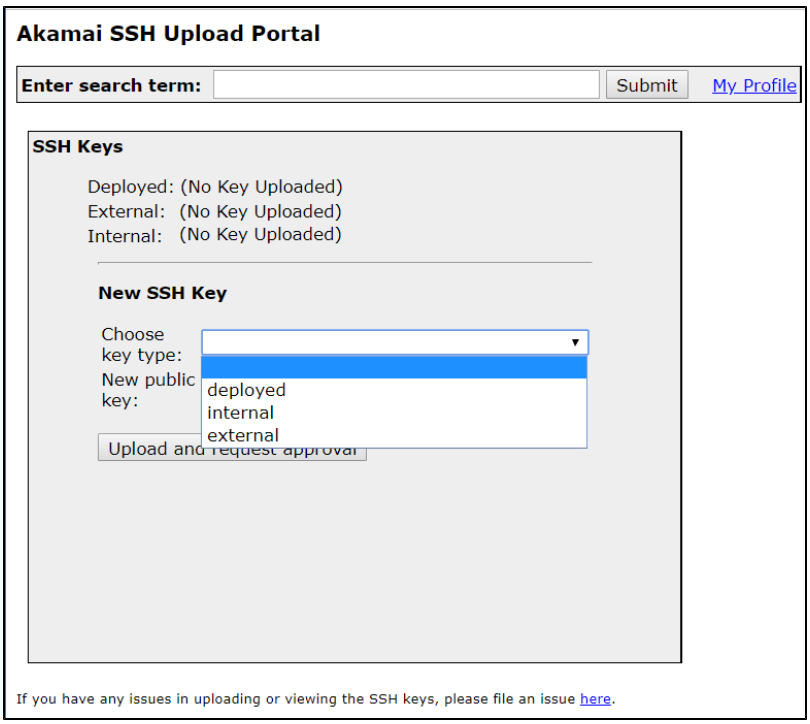
The private half of each key pair is the file that ends with .ppk while the public half is the file that ends with .pub. The file without an extension is a private key (same as the one with the .ppk extension) but in OpenSSH format. The public is the half that will live on the remote server you're looking to access. When you present your private half, the server will unlock because the two halves will match. In order to get the public half of your key on remote servers, you'll need to first upload and verify your keys with the NOCC. You will use the OpenSSH private key on Linux machines to access test networks for labs and development.

Upload and Verify Keys

Upload

1. Access the key upload page, either
    a. From Aloha Quick Links Akamai Contacts Upload SSH Keys (link under your photo)
    b. Or directly here: https://sshkeys.akamai.com/
2. Choose the key type (internal, external or deployed). Protected keys have a separate procedure.
3. Use the choose file dialog box to choose the applicable public key (file ending in .pub)
4. Click on the "Upload and request approval" button.





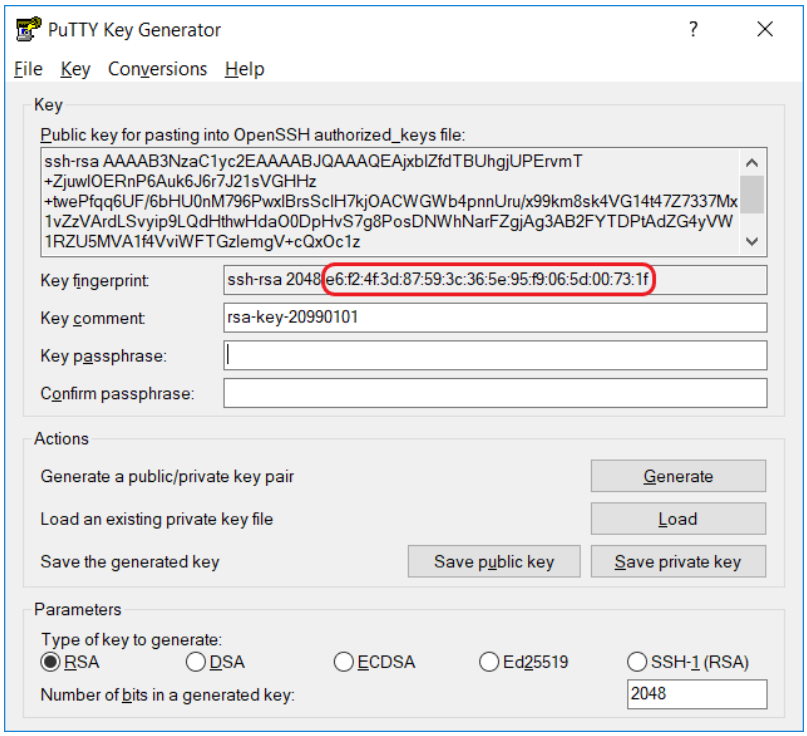
Verify

Once your key has been uploaded you'l receive two emails. The first email will be a confirmation email, the second is a message that indicates your key is ready for verification.

Your key has a unique *fingerprint* that you will need to provide to the NOCC (or the automated key rotation service for subsequent key generations) in order to verify your identity and have the key approved. The fingerprint is shown in the PuTTYgen key fingerprint window when you create your key, but you may need to find the fingerprint again.

To display your fingerprint, load the key into PuTTYgen (Load button next to the "Load an existing private key file" instructions). You will need to enter the key's passphrase to load it.

The fingerprint is the hexadecimal string, what is called an MD5 digest, following the "ssh-rsa 2048" text.

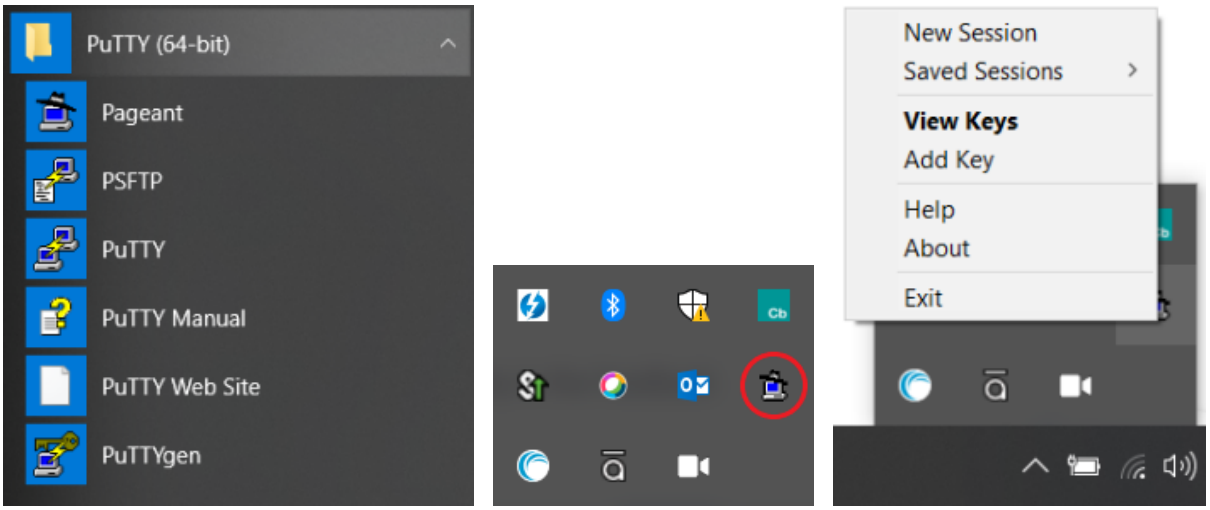


Once you get the fingerprint, call the NOCC at (617) 444-3007 and let them know you are generating keys. You will be asked to read the fingerprint to them, which completes the verification. It may take a few hours for your keys to become effective as your keys propagate through the network.

Add Keys to Session

Use Pageant, the PuTTY authentication agent, to add keys to your session. As with all steps of this lab, you will repeat this for each type of key you want to add: internal, external and/or deployed.

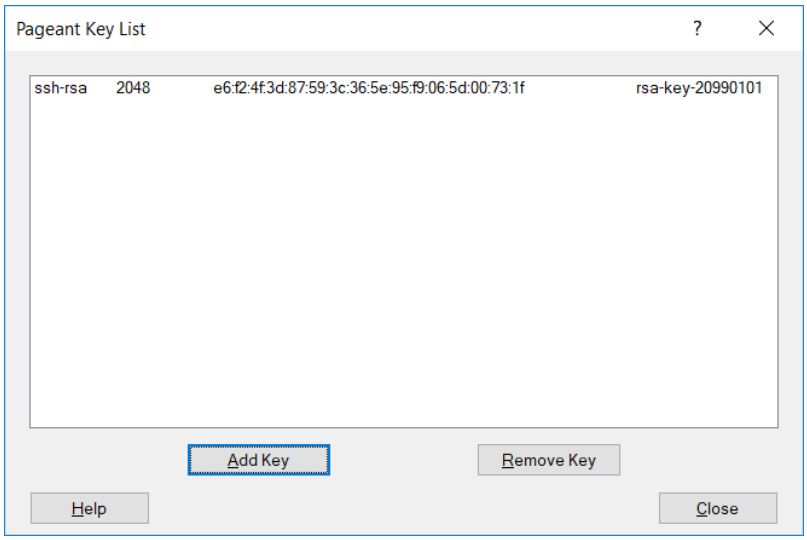
Note: You will add the Windows keys, not the OpenSSH keys!



Pageant is accessible via the system tray with the carat icon (^) at the lower right corner of your screen in the Windows task bar. Right click on the Pageant icon to see the menu. You can click on either "Add Key" or "View Keys" where you are also able to add them.

"Add Key" gives you a file dialog box. Navigate to the C:\ssh_keys directory and select the private key file you want to add to your session. You will be prompted for that key's passphrase.

You can then use "View Keys" to view each key's format (ssh-rsa 2048), the MD5 digest, and the comment you entered when creating the key. Note the "Add Key" button in this window allowing you to add another key to the session as if you selected the "Add Key" menu item above."



Conclusion

Review Objectives

Please review the lab's objectives and verify you have met them by checking off each one. If you were unable to meet any of the objectives, please describe which one(s) you could not meet and why in the Feedback section.

- [ ] Generate public and private SSH key pairs.
- [ ] Upload your public keys and have them verified by the NOCC.
- [ ] Add your keys to your session.

Feedback

If you have any questions, comments or feedback, please send an e-mail to <EngLearnFeedback>@akamai.com.