SSH Key Naming Convention

This page describes a good naming convention for SSH keys, that makes them easier to track, rotate, and revoke.

You should use this naming convention for the filename of keys.
And as well, use the same convention when populating the the comment field of each key.

Here are some design choices for SSH key naming:

- SSH keys are a client-centric object. So, the name should be client-centric.
  Specifically, the name should include the username (actual user or service name).
- To more easily track key usage, the name should include the client machine, where it is installed.
- To know how old a key is (for expiry purposes), the name should include the creation date.
- Since key algorithms can become compromised or superceded by newer ones, some distros and services will refuse certain key types.
  So, we will include the key algo in the name.

The composite key name convention becomes this:

<keytype>-<username>-<client>-<date>

Here is an example of this key naming:

RSA2048-glwhite-hadron-20220428

The above key name expression has the following terms:

1. Key type - what encryption type was used and key strength
2. User Name - associates a key to a single user, for proper authentication and access authorization
3. Client device - associates a key to a device, so the key can be revoked if the device is compromised
4. Creation timestamp - marks when the key was created, so older versions can be identified and revoked

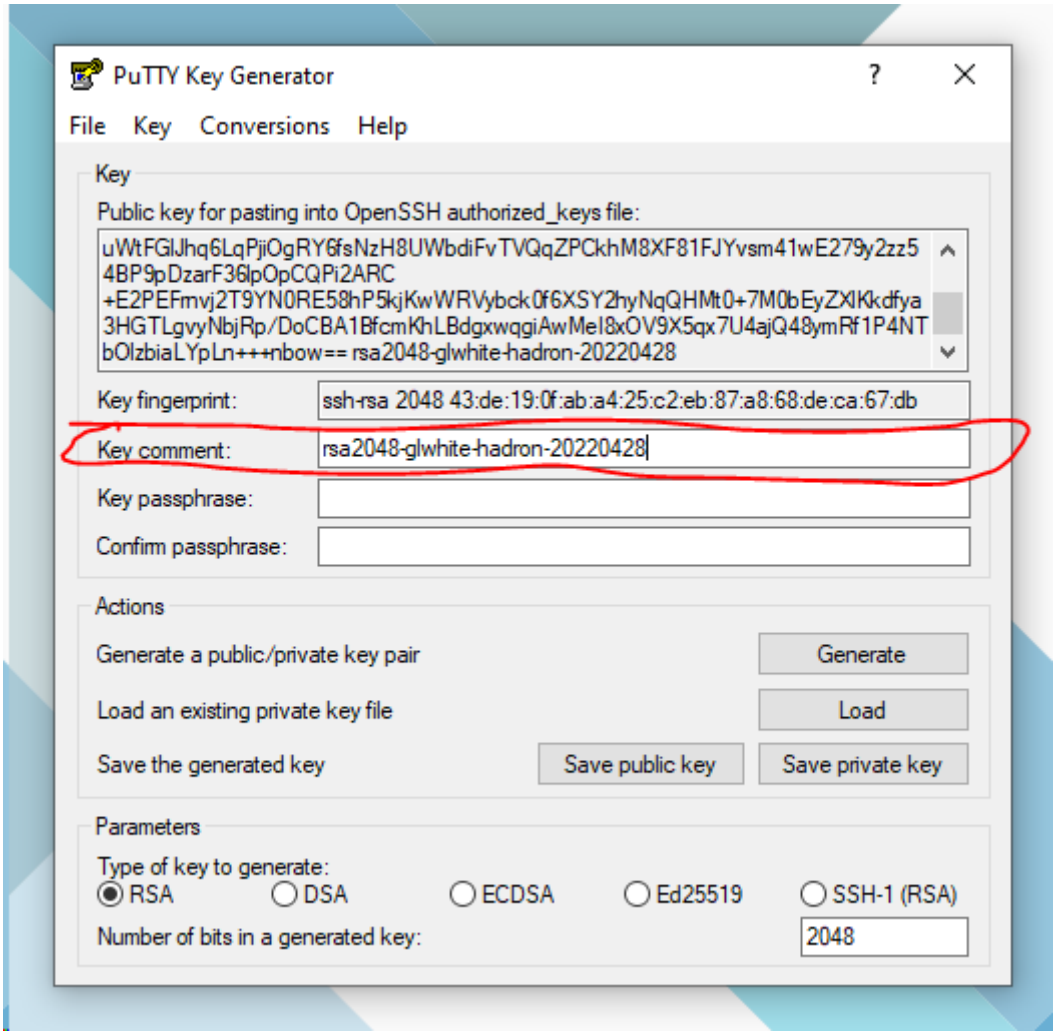
Following this convention allows use to easily identify keys that need to be revoked. As we can revoke keys by device, by user, or by type as a particular encryption becomes obsolete.

As well, the creation time allows us to know when to periodically rotate keys, to limit risk.

The key name should be used as the key comment at the end of a key string in an SSH key file on a server.

The key name should be part of both the private and public key file names (ppk files) on a client machine.

The key name can be set as the Key Comment when generating a key, using PuttyGen, like this:



When PuttyGen creates a key, both the private key and public keys should be saved to disk.

A password can be added to the private key, from within PuttyGen, to prevent unauthorized usage.

If the private key is saved without a password, be sure to store it in a safe bag or in an encrypted volume.

The public key can be stored and distributed without concern.

> NOTE: We've purposely kept the creation time as the last term. This ensures that any automation used to rotate keys can successfully identify the timestamp for all keys (by looking at the last term).

Definite Purpose Keys

There are scenarios that require an ssh key for a definite purpose, such as authentication to a service, such as Github.

In this scenario, it is wise to include the service as a term in the ssh key name and key comment.

Doing so, extends the key naming convention to:

<keytype>-<username>-<client>-<purpose>-<date>

Here is an example of this key naming:

RSA2048-glwhite-hadron-github-20220428

Revision #3
Created 1 August 2025 07:35:34 by glwhite
Updated 1 August 2025 09:00:21 by glwhite