

8.7.3. Generating Key Pairs

If you do not want to enter your password every time you use **ssh**, **scp**, or **sftp** to connect to a remote machine, you can generate an authorization key pair.

Keys must be generated for each user. To generate keys for a user, use the following steps as the user who wants to connect to remote machines. If you complete the steps as root, only root will be able to use the keys.

Starting with OpenSSH version 3.0, `~/.ssh/authorized_keys2`, `~/.ssh/known_hosts2`, and `/etc/ssh/ssh_known_hosts2` are obsolete. SSH Protocol 1 and 2 share the `~/.ssh/authorized_keys`, `~/.ssh/known_hosts`, and `/etc/ssh/ssh_known_hosts` files.

Fedora 12 uses SSH Protocol 2 and RSA keys by default.

Tip

If you reinstall and want to save your generated key pair, backup the `.ssh` directory in your home directory. After reinstalling, copy this directory back to your home directory. This process can be done for all users on your system, including root.

8.7.3.1. Generating an RSA Key Pair for Version 2

Use the following steps to generate an RSA key pair for version 2 of the SSH protocol. This is the default starting with OpenSSH 2.9.

1. To generate an RSA key pair to work with version 2 of the protocol, type the following command at a shell prompt:

```
ssh-keygen -t rsa
```

Accept the default file location of `~/.ssh/id_rsa`. Enter a passphrase different from your account password and confirm it by entering it again.

The public key is written to `~/.ssh/id_rsa.pub`. The private key is written to `~/.ssh/id_rsa`. Never distribute your private key to anyone.

2. Change the permissions of the `.ssh` directory using the following command:

```
chmod 755 ~/.ssh
```

3. Copy the contents of `~/.ssh/id_rsa.pub` into the file `~/.ssh/authorized_keys` on the machine to which you want to connect. If the file `~/.ssh/authorized_keys` exist, append the contents of the file `~/.ssh/id_rsa.pub` to the file `~/.ssh/authorized_keys` on the other machine.

4. Change the permissions of the `authorized_keys` file using the following command:

```
chmod 644 ~/.ssh/authorized_keys
```

5. If you are running GNOME or are running in a graphical desktop with GTK2+ libraries installed, skip to [Section 8.7.3.4, “Configuring ssh-agent with a GUI”](#). If you are not running the X Window System, skip to [Section 8.7.3.5, “Configuring ssh-agent”](#).