**Connecting to a Remote Server with Public/Private Keys**

In this exercise, you create a public/private key pair to log in to the server2 host. If

no remote host is available, you can use localhost as an alternative to verify the procedure.

**1.** On server1, open a root shell.

**2.** Type **ssh-keygen** . When asked whether you want to use a passphrase, press

**Enter** to use the passphrase-less setup.

**3.** When asked for the filename in which to store the (private) key, accept the

default filename ~/.ssh/id\_rsa.

**4.** When asked to enter a passphrase, press **Enter** twice.

**5.** The private key will now be written to the ~/.ssh/id\_rsa file and the public key

is written to the ~/.ssh/id\_rsa.pub file.

**6.** Use **ssh-copy-id -i ~/.ssh/id\_rsa.pub**  **user@ server2** to copy the public key you have just created over to

server2. You are then asked for the password on the remote server one last time.

**7.** After copying the public key, verify that it can actually be used for authentication.

To do this, type **ssh server2** . You should now authenticate without having

to enter the password for the remote user account.